ORGANISATION EUROPEENNE
POUR LA SECURITE DE LA NAVIGATION AERIENNE

CENTRE EXPERIMENTAL EUROCONTROL

LA TRANSPARENCE EN QUESTIONS : LES INCIDENTS DANS LE CONTRÔLE DE LA NAVIGATION AERIENNE

Rapport CEE No. 378

Projet SAF-M-E3

Publication : Décembre 2002

REPORT DOCUMENTATION PAGE

<table>
<tr><td colspan="3">Reference:
EEC Report No. 378</td><td colspan="4">Security Classification:
Unclassified</td></tr>
<tr><td colspan="3">Originator:
EEC - SAF
(Safety)</td><td colspan="4">Originator (Corporate Author) Name/Location:
EUROCONTROL Experimental Centre
Centre de Bois des Bordes
B.P.15
F – 91222 Brétigny-sur-Orge CEDEX
FRANCE
Telephone : +33 (0)1 69 88 75 00</td></tr>
<tr><td colspan="3">Sponsor:
EATMP - SQS</td><td colspan="4">Sponsor (Contract Authority) Name/Location:
EUROCONTROL Agency
Rue de la Fusée, 96
B –1130 BRUXELLES
Telephone : +32 2 729 9011</td></tr>
<tr><td colspan="7">TITLE:
LA TRANSPARENCE EN QUESTIONS :
LES INCIDENTS DANS LE CONTRÔLE DE LA NAVIGATION AÉRIENNE</td></tr>
<tr><td>Author
Ch. FASSERT</td><td>Date
12/02</td><td>Pages
xxv + 70</td><td>Figures
-</td><td>Tables
-</td><td>Appendix
-</td><td>References
61</td></tr>
<tr><td></td><td colspan="2">Project
SAF-M-E3</td><td colspan="2">Task No. Sponsor</td><td colspan="2">Period
2001</td></tr>
<tr><td colspan="7">Distribution Statement:
(a) Controlled by: Head of SAF
(b) Special Limitations: None
(c) Copy to NTIS: ~~YES~~ / NO</td></tr>
<tr><td colspan="7">Descriptors (keywords):

Transparency – Safety Management – ATM – Visibility of incidents – Sociology</td></tr>
<tr><td colspan="7">Abstract:

This report is a summary of the results of a research project carried out in 2001 at the SAFETY Business Area of EUROCONTROL, dealing with transparency in high risks organisations and the visibility of incidents in the ATM domain.</td></tr>
</table>

TABLE DES MATIERES

Page intentionnellement blanche

AVANT-PROPOS

Depuis quelques années, l'ATM en Europe cherche à développer et améliorer ses systèmes et processus de gestion de la sécurité.

L'un des enjeux au début de ce processus d'amélioration est de rendre plus visibles et plus explicites les constituants du système de sécurité de l'ATM ainsi que les risques auxquels ce système doit apporter une réponse. Le passage d'un mode de fonctionnement où la sécurité est implicite - puisqu'elle est la raison d'être de l'ATM – à un mode où la gestion de la sécurité devient explicite, est un passage difficile pour tous les acteurs de l'ATM.
En particulier au niveau organisationnel - pour les ATS providers et les organismes de régulation - les enjeux peuvent s'appréhender à travers la problématique de la transparence des organisations vis-à-vis du public, des régulateurs et de leur propre business, et du "bon" niveau de transparence à établir.

Déblayer cette problématique pour tenter d'appréhender les enjeux, les risques, les conditions et les bénéfices de la transparence par rapport à la sécurité dans l'ATM est le sujet de ce document d'étude.

N. PILON
EUROCONTROL
Safety Business Area Manager

RÉSUMÉ

Ce mémoire est le résultat d'une première année de recherches dans le cadre d'un PhD en Sociologie sur la "Transparence dans des Organisations à hauts risques", effectué à la Sorbonne (Paris) et sponsorisé par Eurocontrol.

Débuté en novembre 2000, cette première année d'études a permis d'explorer le concept de transparence dans ses diverses dimensions (politiques, juridiques, sociologiques) et d'en distinguer 3 aspects :

- l'auto-transparence (processus par lequel une organisation analyse ses propres risques)
- la transparence de l'individu (par rapport à une hiérarchie, à l'état, …)
- la transparence de l'organisation (degré requis de transparence pour instaurer la confiance de l'opinion publique)

Une partie appliquée de cette recherche se focalise essentiellement sur la sécurité dans le contrôle de la navigation aérienne; un rapide point de comparaison a été effectué avec le monde du trading, et le rôle des nouvelles techniques dans ce domaine de la transparence (dont l'outil ASMT, ATM Safety Monitoring Tool est un exemple) est également abordé. Une étude comparative des organisations ATM en Europe a été menée au Danemark, en Italie, en Slovaquie, en Suède et en France et démontre que les pratiques concernant la collecte des incidents varie beaucoup en fonction du contexte national et des différentes organisations. On s'intéresse aussi au rôle joué par le développement du réglementaire qui se met en place au niveau Européen et à son impact sur les pratiques liées à la sécurité.

ENGLISH TRANSLATION

FOREWORD

For several years now, ATM in Europe has been trying to develop and to improve its systems and process of safety management.

One of the stakes at the beginning of this process of improvement is to make the components of the ATM safety system more visible and more explicit as well as the risks to which this system should bring an answer.

The passage from a mode of functioning where safety is implicit, as it is the “raison d’être” of ATM, to a method where safety management becomes explicit, is a difficult transition for all ATM actors.

In particular at the organisational level, for ATS providers and regulatory authorities, the difficulties at stake can be approached through the problem of transparency of an organisation with regard to the public, the regulators and their own business and the “good” level of transparency to establish.

Clear the ground of this issue, try to approach the stakes, the risks, the conditions and profits of transparency in relation to ATM safety is the subject of this document.

N. PILON
EUROCONTROL
Safety Business Area Manager

SUMMARY

This memory report is the result of the first year of researches of a sociology PhD on 'Transparency in high risks organisations", carried out at the Sorbonne in Paris and sponsored by Eurocontrol.

Started in November 2000, this first year of study has been used to explore the concept of transparency in its different dimensions (political, legal, sociological) and to distinguish three aspects:

- Self-transparency (process by which an organisation analyses its own risks)
- Transparency of the individual (with regard to a hierarchy, state authorities, …)
- Transparency of the organisation (necessity and limits of transparency towards public in order to establish trust.

An applied aspect of the research concentrates mainly on the safety in air traffic control, a short comparison has been made with the trading domain and the role of new techniques with regard to transparency (ASMT, ATM Safety monitoring tool, for instance) has been analysed.

A comparative study of ATM organisations in Europe has been done in Denmark, Italy, Slovakia, Sweden and France and shows, that the practices concerning the collection of incident data vary a lot according to national contexts and the different organisations. One is also interested in the role played by the development of the statutory which is set up at the European level and at its impact on the practices connected to safety.

1. Introduction

This report presents a summary of the results of a research project carried out last year at the Safety Business Area at the Bretigny Experimental Center. This study was conducted within the framework of a master's degree in Sociology at the Sorbonne University in Paris, France.

The study began with a theoretical overview: the goal was to question and explore the notion of transparency in various domains (political science, philosophy, law) in order to identify the main questions linked to the emergence of this concept and its increasingly popular use (to the extent that, last year, it became, a kind of buzz-word in the French press). This theoretical aspect is very briefly covered in this report which focuses more on summarizing the *applied* aspects of the research : (1) what are the specific questions raised when we deal with transparency in high risks organisations, and, (2) applying this transparency concept, what can be said concerning the visibility of incidents in the ATM domain?

2. A brief summary of the concept of transparency

In political science, the notion of transparency is now at the heart of the political analysis of institutions. It is seen mainly as a regulation principle ("*Transparency plays the role of a reference myth for the whole set of systems of Power*[1]" said Professor Rideau). Transparency seems to lie somewhere between a principle and a virtue, and the difficulty of defining it in precise terms is such that Transparency is sometimes considered to be one of these "soft" notions (Lequesne[2], 1999), that are overused in our democracies (e.g. : subsidiarity, assessment, etc.)

A legal approach provides a more operational definition:Transparency is always the transparency of "something" with regard to "someone»: laws on transparency always apply to a concrete contents and determine a balance of powers *(who* is entitled to see *what*). Lassalle[3], for example, considers that Transparency became one of the central values promoted by American democracy with the promulgation, in 1966, of the Freedom of Information Act. President Johnson, on the day of the promulgation of this act, declared that "*a democracy can be effective only if citizens have access to all the information compatible with state safety*".

The concept's recent vogue and, perhaps also, its overuse in the press in many different domains (economical, administrative, financial, political, etc.), has raised some concerns over the dangers linked to an exaggerated focus on transparency. Guy Carcassonne[4] criticises the fact that transparency may be seen, sometimes, as an end in itself. He reminds us that "*transparency is a means, like others and amongst others, to attain the superior objectives that spring from the idea of democracy*". And he adds : "*Its usefulness, as its legitimacy, must be gauged according to the objectives that it serves*".

Mirroring this vision of transparency as a tool for democracy is the issue of how *individuals* are made visible to an *organisation* (this organisation being a government or any kind of institution). One of the first descriptions of this process is found in Foucault (*Discipline and punishment, the birth of the prison*, 1975). Foucault defines the Panoptic as a mechanism of control and "visibility" of individuals. In his evocation of Bentham's "panopticon", he proposes a symbolic model: a tower surrounded by a ring, divided into cells, with windows opening on the inner face of the ring, the other, outer, allowing daylight to pass through the whole cell, in such a way that the shadows of the occupants can be seen in black light. This can be seen as the architectural principle of a form of transparency, as stated by Foucault: "*in the famous cage, transparent and circular, with its high tower, powerful and erudite*".

The fear of a society that would make all citizens "visible" to a central power is emerging as a response to the increasing use of new techniques that facilitate various forms of invasion of privacy. Very popular in the development of a rhetoric that is critical of these new dangers, the reference to Orwell and his "Big Brother is watching you" is now classical. In recent years, the "Big Brother Awards" of the NGO Privacy International have given prizes to the government and private sector organisations, which have done the most to threaten

[1] Quoted by Noelle Lenoir. Conclusion. Actes du colloque organisé par le CEDORE (Nice) sur "*La transparence dans l'Union européenne. Mythe ou principe juridique ?*" L.G.D.J. 1999.
[2] *La transparence, vice ou vertu des démocraties*, Christian Lequesne. Actes du colloque organisé par le CEDORE (Nice) sur "La transparence dans l'Union européenne. Mythe ou principe juridique ?" 1999. "L.G.D.J."
[3] Lassalle. *La Démocratie américaine*. Colin, 1991.
[4] Guy Carcassonne. *Le trouble de la transparence*. POUVOIRS, n°97. avril 2001, Seuil.

3. Transparency in High-risk Organisations and Trust

An exploration of the relations between transparency and trust is another dimension of our study. It is clear that, as the above political frame of reference has already demonstrated, there is a link between transparency – some kind of visibility from the outside - and trust. The underlying question, which is raised here, could be: *How much does an organisation have to be transparent to gain the public's trust?*

A German sociologist, Simmel, has given a very simple and elegant definition of Trust.

Trust is also an intermediary state between knowledge and absence of knowledge. He who knows all doesn't need trust, he who knows nothing can't reasonably trust.

Simmel wrote this at the end of the 19th century. He added to this another important idea: the fact that *culture* has progressively established a clear quantum of knowledge and non-knowledge that are necessary to trust in most social situations and work relationships.

But what may have been true at the end of the 19th century is certainly not as simple to set forward in our modern world which is more complex and more unpredictable as shown in the classical analysis of H. Arendt in "the Human condition[6]". And it is definitely a challenge to decide, in the field of high risks, what is the necessary *quantum of knowledge* for building trust. Or, in other terms, what should citizens know to reasonably trust those fields that involve high risks?

One classical solution is to establish regulation authorities that stand as an interface between the service provider, nuclear industry or air traffic services, for example, and the public. But this simply results in shifting the same question to another location: what should a regulation authority know about the organisation it regulates? There is no easy answer and we know, for example, that regulation styles vary significantly between countries. This was shown, for example, by Gene Rochlin in his comparison of regulation styles in France and in the USA in the nuclear domain. Moreover, the role and efficiency of a regulation authority whose purpose is to control high-risk activities is certainly not easy to define. Diane Vaughan, in her analysis of the Challenger catastrophe has shown that the internal and external regulatory authorities for NASA were not able to play this screening role: they failed in identifying the risk linked to the booster, which provoked the catastrophe. And, according to Vaughan, the reason was mainly linked to the fact that the regulatory authorities, to some extent, looked at the problems with the same magnifying glass that the NASA itself was using to examine its risks, and, consequently, they were not able to identify a risk that NASA itself had not identified.

In the field of air traffic management, the Safety Regulation Commission has launched a survey of the ATM contribution on aeronautical incidents and accidents in Europe (Blaize, 1999). Are incidents known and visible within ATC providers? Are they made visible to the regulator? The conclusion of the survey states: "it has been found that limited safety data exists for ATM-related incidents other than AIRPROX". Not surprisingly, the report also reveals discrepancies as to the visibility of incidents within different countries. Some ATC services have no AIRPROX at all. Are they safe or are they a bit too opaque? The applied part of this research involves a comparative study led in several European countries.

[6] Hannah Arendt. La condition de l'homme moderne. AGORA, Calmann Levy. 1983.

4. The Case of Air Traffic Control

A comparative study allowed us to examine several ATM organisations and their processes of collecting and analysing incidents. This first analysis enabled us to raise a few important questions. The ATM organisations examined are located in Sweden, France, Slovakia, Italy and Denmark. In order to preserve the confidentiality of the persons interviewed, only basic characteristics of the individuals' work are signalled (e.g., "a person in charge of safety") , without details on his/her exact position.

4.1. What events are analysed?

There exist a great variety of technical and human means that make it possible to collect events, signals and incidents. These include, from the airline company's point of view, ASRs, TCAS events, FOQA type programs and AIRPROX and from the point of view of air traffic control, incident reports or the AIRPROX of certain countries. Even the criteria of "that which is worthy of examination" varies according to each organisation's understanding of safety. We encounter here a good illustration of Weick's notion of *sensemaking*: the choice of what subjects should be examined isn't a universally *understood process*: it is *a construction of the organisation*.

Secondly, at a purely quantitative level, the more means we dispose of, the more we can collect incidents, but also, and more significantly, the more we develop alarm mechanisms (such as the FDS or the TCAS) the more things we can "see."

Thirdly, the characteristics of the collection process will depend on elements particular to the ATM organisation (its tools, the structure, when existent, of a safety management service, etc.), or to the airline company (that will have its own AIRPROX declaration practices). It will also depend on much more macroscopic elements, such as the punitive (or non-punitive) character of the laws concerned with sanctioning professional error in each country. It seems, however, that the general tendency in the four countries studied is data collection focused on AIRPROX.

4.2. Obstacles to the reporting of incidents

There now exists a consensus on the insufficiency of AIRPROX data and on the need to obtain other types of information through a cross-disciplinary approach that takes in the various theories in the fields of engineering and safety. In this light, examining the obstacles to the reporting of incidents can be particularly useful. Here are a few examples that are in no way exhaustive:

4.2.1. A legal obstacle

Denmark provides a particularly salient illustration of the impact of macroscopic factors on transparency within an organisation.
Until July 1, 2001, Danish Aviation Law made it possible to fine a controller who had had an incident. Cancellation of license and, in extreme cases, prison sentences were prescribed. The DATCA (the Danish air traffic control union) initiated the revision of this law. Their arguments against the law were rooted in a classic safety engineering rationale: the need to know incidents so as to get feedback from experience. Few incidents were being reported and reports were generally limited to cases in which the "other party" (pilots for controllers

and vice versa) was to blame. For a long time, the administration congratulated itself on the apparent "good safety" demonstrated by the small number of official incidents.

Thus, there exists an indisputable link between laws of a punitive nature and the non-transparency of incidents within an organisation. Beyond the concrete nature of the punishments received, it is the absurdity of a law that is useless from a safety point of view that has been underlined by the Danish controllers.

The law's revision, initiated by the Danish air traffic controller's union, was brought about by involving the various media in a public debate (e.g., with television programs and numerous articles in the press). This stimulated the involvement of Danish citizenry as a whole in a reflection on justice and safety in big systems.

Debates focused on the fair or unfair character of a measure that could concern controllers and bypass other professionals such as medical doctors. In the end, negotiations resulted in a guarantee of transparency obtained in exchange for the abolition of the punitive character of the law. Controllers are now required to report their incidents[7], and these incidents (in which the individuals involved remain anonymous) are made public in compliance with the "Freedom of Information Law." Thus, the transparency that is taking hold in Denmark is a negotiated transparency, providing an original example of a debate framework in which the professionals of a high-risk organisation and simple citizens can discuss issues together and find solutions.

4.2.2. A structural obstacle

We can easily understand why a controller conceals incidents in a country that penalises errors, but there are many other obstacles to the reporting of incidents, only a few of which we will explore here. One important obstacle is the lack of real encouragement to make reports: the lack of structures, of intermediaries, of feedback (why fill out all the paperwork when there are no tangible results?). Another, related, obstacle is the absence of meaning given to the incident by the organisation. As Mrs Helle Münsko, who directs the Danish controllers' union, explains:

> *But there were also other reasons for not reporting.One is the fear of being fined, another is the "loss of face", because the old culture was that we don't make mistakes, and yet another explanation is that reports were not used in any proactive way at all. I think that we could have lived with the fine (or worse) if only the reports were also used for something else, so as to prevent the same thing from happening again. But the reports were only used to place blame. And another factor was definitely a very long and slow investigation process. We have several examples of cases, which have taken 2 years to investigate - only to find out that the controller was to blame and had to be fined. No other recommendations came out. This has also been a reason for not reporting. It is a very demanding task and very destructive to any human being to live in uncertainty for so long.*

In certain cases, error is still experienced as a sort of taboo, including within the air traffic control teams:

> *No, no one confesses to having made an error. It's a sort of… It's difficult to say, yes, it's difficult to say ' it's me who made the error.' That's hard to say. (Slovakian controller)*

[7] In conformity with a EUROCONTROL directive (ESSAR2)

Inversely, in Sweden, the reporting of incidents is, globally, a routine part of a controller's activities. On a number of occasions, the individuals interviewed insisted on the "non-reprimanding" character of investigations. Marlene Dyrløv Madsen and Thomas Ryan Jensen[8], who compared analyses of Danish and Swedish incidents, noted a choice of very neutral wording in the Swedish reports, which, rather than containing value judgements regarding actions or decisions taken by controllers, endeavoured instead to identify the mechanisms of error in cognitive terms, then placed them within a systemic view.

4.2.3. A symbolic obstacle

As the CETCOPRA has pointed out, pilots and controllers have an ambivalent relationship[9]. Though pilots' (and more frequently air line companies') complaints regarding controllers are well known (notorious delays linked to air traffic control occasionally result in captains making sarcastic announcements to their passengers), a certain form of solidarity remains alive.

This solidarity can be at odds with the fact that when a controller reports an incident this can, in certain cases, bring to light an error or a procedural violation on the part of the flight crew. Rather than being part of a Feedback from experience process or revealing a dysfunctional mechanism, the reporting is seen as being an act of "treason" towards a colleague. A person in charge of safety brings this point home:

> *Do you know Nice? These were pilots that turned left while taking off towards the north -east, in other words directly towards the city and the mountains, and, of course, in bad weather. So the controller in question said "I got blamed for that one." But I didn't just leave it at that. I called up Nice and, finally, there was a little investigation and I realised that there had been three similar and unknown cases of people who'd turned left. These were cases where there could've been an accident. These were twin engines that went up pretty quickly but with a four engine aircraft they wouldn't make it above the mountains. We ended up realising that it was linked to a trap in the Jeppesen maps, at three hundred feet a right-wing turn following a certain course, and on one of the standards (SID), another map. This map presumed that you had the Jeppesen… and so on this map it was "turn left" to get to a particular beacon. And so, in this case, you had people who'd only taken the SID map where there was no reminder that first you had to turn right… And so an important problem remained hidden because the controllers didn't want to denounce the pilots. This notion of denunciation prevents… I would say the reporting of anything that isn't "loss of separation" …*
>
> *So if we take this example of Nice, it's not to hide things: it's to avoid causing people problems… OK, from time to time the controller is responsible, that's obvious, but, most often, it's a pilot-type error and controllers don't want to report it.*

But there is hardly a systematic consensus among controllers on keeping secrets closely guarded within the pilot/controller community. Between the secret as positive value and the secret as risk factor, some will lean toward the second interpretation. But how does one talk about incidents in an organisation that doesn't necessarily provide the structures and the

[8] Marlene Dyrløv Madsen & Thomas Ryan Jensen*: Fejl, ansvar og moral: Behandling af menneskelige fejl og udvikling af en professionsetik inden for flyveledelse og andre sikkerhedskritiske områder*. Technical Report R-1260, Risø National Laboratory, 4000 Roskilde Denmark. 2001.

[9] Gras, Alain, Moricot, Caroline, Poirot-Delpech, Sophie, Scardigli, Victor. *Face à l'automate : le pilote, le contrôleur, et l'ingénieur.* Publications de la Sorbonne, 1994.

practices that would make reporting a "non-denunciatory" action? In certain cases, one has to step out of the institutional framework. Total publicity can result:

> *There was a serious incident in which a foreign company descended at 4 or 5 nautical miles from Lyon and so really just about hit the hills when you're facing north. A controller took note, the alarm[10] was identified. It happened on a Friday and then on Tuesday nothing had been done, or else it had remained blocked… Then on Wednesday there was an article in the local paper and, judging by the contents, we have a strong suspicion that it's one of the controllers there that doesn't think it's normal to bury something like that.This is a very interesting event in terms of Feedback from experience (a French person in charge of safety).*

4.3. What sort of external transparency ?

In this chapter we will consider an organisation's perception of "its" transparency with regard to reglementary authority or to the public in general, etc. Our object is to explore the spontaneous self-appreciation of agents of a high-risk organisation when we deal with this issue, whether they are controllers or safety managers.

4.3.1. Admitting that a controller is taking risks?

While discussing the subject of transparency, an Italian controller spontaneously brings up two obstacles, complexity and risk-taking, the second of these being considered "too shameful to mention." The following is an excerpt from a discussion with two controllers:

> *Question: I'm doing research on transparency. What is hidden? What is shown?*
>
> *Answer: Very little is shown because it is difficult to explain to people what our work is, what is our job, and for instance safety, how you can explain … you work and something can go wrong, or something can go OK, so if you are quite sure that something goes OK, you accept the thing, but you are not sure it is OK, so you accept the risk, it is a very very little risk, but you accept it, so how can you explain this to a person going aboard an aeroplane, to the passenger.*

The second controller adds: *the passenger thinks there is no risk, but it is not true …*

That passengers think there's no risk is certainly arguable[11]. That certain passengers are afraid to fly is a well-known fact. However, what the controller points out in an interesting way is that these types of micro-regulations (not everything is anticipated, covered by procedures, and the controller has to manage an acceptable margin of risk) are very difficult to explain to the public. Here, again, we encounter the problem of Simmel's "quantum of information necessary for trust": the public *must* trust regulations that it can't understand for they demand an excessively detailed understanding of the professional's work.

[10] The MSAW (Minimum Safe Altitude Warning) alarm

[11] Christine Noiville has observed that "the public is more after "zero contempt" than "zero scorn"; information and trust thus play an essential role in forming an individual judgement on risk", *Le risque acceptable, une vision juridique,* Colloque CNRS Risques collectifs et situations de crise, Février 2000.

4.3.2. What should be transparent?

The transparency of incident data evolves.

> *I think that Eurocontrol has had an important impact.Until '94, '95 there was no management of the safety part of Eurocontrol. There was the first safety meeting, it was called the SMITF at the time: Safety Monitoring Improvement Task Force.It was the embryo of what is now the SISG (Safety Improvement Sub-Group).You see, countries didn't have the habit of managing, of talking about safety together, nor between themselves and Eurocontrol and so, finally, unaware of what was being done, of what was being undertaken by one's neighbours, we would hide [incidents]. Then the SISG, or rather the SMITF was created. We were three countries to begin with: the English were already there, us, the French, and the third, I think, were the Swedish. Afterwards there was a Dutchman: it took a while to get going.(…) When you see the neighbour doing it, since he gives me his figures, and not just his figures, his methods of calculation and analysis, the big causes, the appraisal. We all did our safety appraisals in front of our neighbours, quite tacitly in fact, while double-checking with our respective administrations. I think this was what was being done; this is what I was doing anyhow. What do we give, what do we hand over, do we censure information or not? Personally I didn't want to [censure] and so I said "it would be good if we could say everything" and, at the time, my direct boss agreed that everything should be said. From that moment on – he'd asked me how it was going, anyhow – we told ourselves "OK, let's go for transparency. It was new, you know, transparency at that time. We're transparent… (…) Anyway, there are 800 TCAS – we're not afraid of saying so. We're a little bit, even a lot less transparent on the causes.*

4.3.3. The limits

Transparency has limits that some individuals underscore vehemently:

> *Are our organisations sufficiently transparent from a safety point of view? No! Let's not beat around the bush, the answer's no. Is safety really a crucial issue? It's a major issue… You see, it's always the same line… (A French person in charge of safety)*

Others adopt a more moderate tone:

> *I would say that transparency… it already has its limits, and it's a concept that we defend when we are capable of mastering safety management.That is to say, we know what we're going to find because we know what tools we have, we know what we're capable of doing with them and we fix ourselves a limit – what I'm telling you is personal – in the disclosure of information we've obtained. I don't really believe in total transparency and what does transparency really mean? Is it being transparent with regard to figures, or to facts, or to analyses, or to effects? In France, for the last two or three years we've been saying "we're transparent." (A French person in charge of safety).*

An example:

> What I've had a tendency to say for the last two years, even if things are getting better, the double runway at Charles de Gaulle, for example; the functioning of the double runway is dangerous. That is, the parallel landing and taking off like that on two runways

that are so close together. It's dangerous because, right now, the methods aren't clearly established. You can't say it, though. Transparency has its limits because we're going to say "Hey Joe, wait, if you say that, well, they'll stop Charles de Gaulle and then what'll happen to us? It isn't fathomable." You see, transparency still has its limits… (a French person in charge of safety)

4.3.4. Evaluating risk

The Safety Regulation Unit asked for incidents to be reported and also for there to be an evaluation of risk for each AIRPROX so as to carry out classifications. The risks are grouped into 5 classes, from A to E, risk A representing the most serious type of risk (the risk of collision). The ESARR document gives precise indications that facilitate the classification process. It has borrowed from French methods. For example, an incident that is below the half-norm usually leads to a risk A classification (except, for instance, if there has been visual separation). Similarly, a justified TCAS RA (Resolution Advisory) will generally lead to an 'A' classification[12]. A French manager explains:

> *You take the same incident analysed by England, France and Italy and you won't have the same risk. I talked with some Englishmen, I told them: how is it that, out of 180 AIRPROX per year, you have 80% where you say "risk nil", while we have only 20% risk nil?! It's actually easy to understand: from the moment that you have a RA TCAS, it comes close to being a RA TCAS… We mark down at least A or B, high risk, while they, in sum, have the opposite reaction.The English say: the RA TCAS was activated, so there was no risk… and that's where Eurocontrol fails to separate the sheep from the goats.*

The SISG group provided an opportunity to compare different countries' practices. The French classification, and the SRC classification that it has inspired, using criteria other than that of the distance of separation between aircraft, leads automatically to the classification of a majority of AIRPROX in A or B, while the NATS classification (that proposes a risk evaluation form that attributes points according to a number of criteria) classes more AIRPROX in C. The NATS presented its classification system, and discussed it with other countries (namely Italy and Germany) that were convinced of the usefulness of this method of risk evaluation. But what of its conformity with ESARR 2?

A discussion in Italy:

> *I have spoken to P. Statsny[13], I told him I did not agree to apply ESARR 2 with this manner, I am aware ESARR 2 is very official, but maybe we could not remove, but integrate. I told him: "When you say ' if the separation is less than X NM or feet, you have to classify in risk "A"', it is an example, only an example?»*

Once convinced by the NATS method, it is necessary to convince the incident analysts to moderate their evaluation of risk that seemed, up to now, to be fairly close to the French manner of doing things. It becomes necessary to "change their brains"!

> *Until 4 months ago, investigators, if you were evaluating an AIRPROX taking into account a lot of topics, but at the end the vertical distance creates something mandatory… with this new procedure, investigators have to modify their old point of view, and to think with another mind, with another brain, it is important before to*

[12] The TCAS is based on temporal data: it is set off 25 seconds before a possible collision of the two aircraft. In the majority of cases, this also corresponds to a distance of separation inferior to the half-norm.
[13] Mr. P. Statsny is head of SRU.

issue this to say to investigators, from now you have to think that if the TCAS RA is blinking, it is not necessary to interpret it as something as "this is a very big AIRPROX, you have to mitigate with the whole cues of the scoring system, that you have to evaluate, you have to balance. (an Italian person in charge of safety).

Recently, the French Air Navigation Administration (DNA) expressed concern over the French figures for the year 2000 compared to those of other countries: they show that French AIRPROX are very serious (many risk 'A's) while many other countries have much less serious AIRPROX ('C' and beneath). This is, anyway, what a quick overview of the statistics given to the SRC seems to indicate[14]. The DNA questioned the appropriateness of publishing these statistics and would like to have a better look at the analyses carried out in other countries.

These debates demonstrate the extent to which the evaluation of risk is constructed within the organisation and the extent to which it is determined by different safety paradigms. These paradigms, in turn, are certainly influenced by the conditions in which the information is rendered public. Some of the countries end up adopting the method of risk evaluation proposed by the NATS, which may well offer a solid base of reflection on what a risk is, but which also, incidentally, leads to AIRPROX being classified in the maximum risk category 'A'.

4.4. Analysis and feedback

4.4.1. Current shortcomings

Specific conceptual and methodological terms for the analysis of incidents are poor if not entirely non-existent.Analysts do their best and, despite the back-up provided by technicians, an important part of their time is devoted to the painstaking task of rewriting frequencies, etc. Among the organisations observed, the Swedish, who remain attached to a systemic vision, are perhaps most inclined to produce refined analyses.

4.4.2. Local Regulations of Risk

The Swedish example (or the Malmö example, to be more precise) shows the value of the local treatment of incidents, with what Cyril Barriquault calls a *short loop* in the Feedback from experience process. The "*events from which we can learn*" are discussed locally, their richness is kept intact thanks to the understanding of context that is maintained, while the coding process of a data base inevitably results in the impoverishment of the information that's retained. After the "*local treatment*" comes the "*local remedy*". The "local remedy" doesn't mean taking earth-shattering decisions that have no place here, or, as Cyril Barriquault's study reminds us, "*minor incidents and, particularly, their control, are part of the normal process of work regulation; they reflect the expertise of the front-line operators who manage the man-machine system's adaptation to context.*" It is, thus, a case of allowing controllers to work on local "self-transparency" which ultimately allows for a better regulation of risk-taking as well as a better regulation of the efficiency of micro-regulations carried out by teams. The reported events can, for instance, make it possible to detect that a small routine violation that everyone does, in a given situation, dangerous, or that a cursory evaluation that is valid in most cases is false with regard to a aircraft's particular performance, etc.

This Swedish solution offers several avenues of reflection on questions that haven't, as yet, been dealt with. With the example of trading, a topic analysed briefly in our study and which isn't detailed in this summary, we saw how a trader's daily practice of "reporting" encouraged each professional to fully explain his/her reasoning, "*because it pushes you to think more on what positions you take, and why"*; and how this effort to be "*more transparent to one's self*" was looked upon as a feature of risk regulation. Where, elsewhere, dialogue takes place between each trader[15] and their "desk" manager, regulation in the Swedish example is carried out collectively, though, of course, both forms of dialogue share the same objective. Nevertheless, this refined regulation of risk isn't any more "publishable" for the controllers than it is for the traders. As the Italian controllers put it, "so you accept the risk, it is a very very little risk, but you accept it, so how can you explain this to a person going aboard an aircraft, to the passenger?" And so, the dream of an organisation that is totally transparent with regard to every event, can give way to the notion of *sufficient transparency* where the treatment of certain events is devolved to the local level.

It seems that organisations that have developed these procedures of local treatment of incidents by front-line operators are also those that already had a very solid organisation in terms of the more classic "Feedback from experience" concept, with the centralised analysis of events, etc. It would be necessary to explore other examples in order to determine whether what we are dealing with is linked to the maturing process of this "learning from experience" concept.

4.4.3. The organisational regulations of risks: setting an agenda

But organisational actions are also necessary. Shortcomings in the functioning of the system are also linked to actions taken at high levels or by international bodies (regulation authorities, for instance). Some concrete examples: controllers' inability, at their level, to modify a procedure that they judge to be dangerous; lack of sufficient training; the reclassification of airspace; relations with airline companies so as to consider the impact of the TCAS on the relation between pilots and controllers, etc. It is what some sociologists have only recently been calling the "agenda setting" of risks. In other words, the collective awareness of a risk and its influence on decisional processes involves the whole

[15] Which is true for the analysis of actions after the event. We saw that there also existed collective regulation, orchestrated by the Desk Chief in real time. cf., Chapter 3 in the main document (in French).

organisation, from the front-line operators to management, and can even be considered to be *interorganisational*, as we will now attempt to demonstrate.

If we briefly examine the example of the fixing of an agenda for the problem of "runway incursions" within the civil aviation community, we can refer to the notions of *structural secret* (Diane Vaughan used this notion in her demonstration of how structural and functional aspects of an entire organisation made it possible to *weaken* the alarm signals with regard to the resistance limits of certain shuttle joints), *strategic decision* (Hervé Laroche examines the process by which problems come to leaders' attention and shows how the dominant paradigm can prevent awareness of a problem) and *sensemaking* (Weick). Let's listen to a French person in charge of safety:

> *The Americans have the "safer sky" initiatives, which identify the most important items. The JAA too. Until a year ago, runway incursions weren't a problem for them. We bugged them on this point.There was awareness that there were some [problems], but they [the problems] weren't known. Now that the director of the JAA has the figures for Roissy (number of RIs per takeoff), they were really stunned because, for them, from the SFACT point of view, these kinds of figures for a critical element would be unthinkable. Roissy is the only place in Europe where we have the figures, thanks to ASRs and controller reporting, we have some, we have quality graphics with the evolution of RIs that are now circulating everywhere even if this earns us the reputation of undisciplined students. But there's no reason why it shouldn't be the same everywhere. So now the JAA has decided to set up a task force in this field. Clearly, people weren't conscious of the problem in this domain. Now that we're conscious, we're beginning to also know the runway incursions outside of Roissy: we must have had 5 or 6. We went from zero to 5 or 6 really quickly!*

It's worth noting that, since very recently, there exists a Eurocontrol "Runway safety initiative."
This notion of agenda setting considers transparency issues in another light, by linking them to decision-making processes. We have seen how artificial it would be to separate the processes of transparency-making (what sort of information do I obtain on my risks and shortcomings) and decision-making (once I've collected information, what do I do with it?) Furthermore, Cyril Barriquault has observed (personal communication, not published) that incident analysts often developed, through experience, a very refined intuition, that by nature is difficult to formalise, for the *very significant* incident that highlights an overlooked aspect of the system's shortcomings. As Hervé Laroche has suggested, we should now be thinking in terms of the "formulation of strategic problems" that take into accounts all of the organisation's levels.

5. Conclusion

This study allowed us to explore the three dimensions of the notion of transparency and to apply them to a concrete problem (the visibility of incidents, the perception of risks) in the field of air traffic control.

We first adopted the self-transparency approach, the dimension that is most emblematic of modernity. When present in a specific organisation, this dimension presents fundamental limits, as Alain Gras has demonstrated with his Macro System Technique, and sociological limits, highlighted by Diane Vaughan with the Challenger example. A critical review of the notion of transparency has made it possible to question an excessively simplistic vision in which transparency is seen as the unveiling of a pre-existing "truth". Breton criticised the shift of meaning that was occurring between "information" and "truth", and Weick's notion of sensemaking enables us to understand the process that creates information and constructs meaning.

This meaning is determined by a dominant paradigm that is constructed collectively but that remains dynamic. The collective construction of what is to be selected is elaborated at all of the organisation's levels. For Hervé Laroche, the paradigm only evolves through trials, but it seems to us that there also exist less revolutionary transformations that are more continuous and that can be brought by deliberations between agents. The next step, then, to follow up on our study, would be to confront the notion of sensemaking (Weick) with that of setting an agenda for problems linked to safety in European civil aviation, applying to this confrontation the problematic of strategic decision-making. For this, it will be necessary to adopt an anthropological approach that combines cognitive, organisational and symbolic elements, and that takes full account of the inter-organisational dimension. Thus, to take the example of risk evaluation for AIRPROX or for runway incursions, it is clear that the following factors are relevant: the perception of front-line operators, pilots and controllers; the role of incident analysts, of safety managers, of the hierarchy of each centre, but also that of groups like the SISG, or such entities as the SRU.

The *transparency of the individual* angle allowed us to explore a paradox that is perhaps only apparent in our society: exaggerated media exploitation of voluntary exposure of self, on one hand, and, as a mirror, increasing criticism of the creation of technical tools that facilitate intrusive forms of exposure of individuals to visibility. Given the problems specific to the field of activity we chose to study, we decided to focus our attention on the second of these two axes. Transparency always implies a form of mediation between powers: Foucault had made Bentham's panopticon "*the diagram of a power mechanism reduced to its ideal form."* In a sociological vision anchored in realities that are, fortunately, less *ideal*, one question remains completely unanswered, that of the limits to individual control that are the result of democratic concerns. Charles Perrow considered that only the total control of individuals by an organisation (that Sagan likened to Goffman's total institution) could ensure the safety of structurally risky systems[16]. But, he declared, "*I do not want to live in a society where we have to do that with nuclear power plants and DNA and a lot of other risky systems."* [17] Others, though in a very different theoretical context, and with a different set of justifications, consider that extreme safety concerns (derive securitaire) aren't necessary and are even undesirable. ???. In defence of the implicit, and, for management, necessarily opaque adjustments piloted by front-line operators we can find Friedberg's "*margin of opacity*", and Amalberti and Barriquault's "*joint piloting of performance, risk and work*

[16] As a reminder, we already explained (in Chapter 3) that Perrow offered a classification that allows him, through the use of the two axes, "coupling" and "complexity", to class industries of varying danger. But he separates "aircraft" and "air traffic control" systems without dealing with any of the aeronautic MST. Which earned him the criticism of Alain Gras.
[17] Risky Organizations and "normal" accidents. Charles Perrow's point of view. Seminar on Collective Risks and crisis situations. Fourteenth meeting

satisfaction." Some degree of privacy in the workplace can and should be maintained, especially if it is accompanied by local practices of Feedback from experience such as those observed in Malmö, Sweden, which permit a "short-loop" regulation of conduct that is determined by the controllers themselves. But this doesn't have to entail a complete shift towards the *opaque autonomy* whose failings and sociological price in the field of nuclear power have been demonstrated by Mathilde Bourrier.Transparency as a form of risk regulation is also a notion that merits further investigation in a future study, as is also the link that the *first-line* professional makes between *his/her* transparency and the meaning given to this value within the organisation, (who else is transparent and what is being done about it?) in the continuation of what has been discussed in the example of trading.

The last dimension of our exploration, that of the *transparency of the organisation*, can't overlook the notion of trust. We demonstrated how plans for "*total transparency*" were, at best, a sort of catch phrase used by a political agent seeking to signal (whether sincerely or not – we can always give him the benefit of the doubt) a change in the management of safety in an industry that no longer inspires trust (as it were). For every organisation has its share of *implicit negotiations* that it would be pointless to try to formalise. Nevertheless, and here lies the dilemma, air traffic control, like other similar organisations, will likely be increasingly obliged to guarantee the "*institutional constancy*" (La Porte) that makes it possible to maintain the public's long-term trust, and thus will have to provide a form of transparency that remains to be determined while keeping in mind Simmel's elegant phrase: *Trust is also an intermediary state between knowledge and absence of knowledge. He who knows all doesn't need trust, he who knows nothing can't reasonably trust*. Christine Noiville's phrase, in which she reminds us that the public doesn't want *zero risk*, but rather *zero contempt*, is in our opinion perfectly emblematic of current challenges.

La transparence en questions :

Les incidents dans le contrôle de la navigation aérienne

Christine Fassert

Mémoire de D.E.A de Philosophie
Option : Socio-Anthropologie des techniques contemporaines

Sous la direction de :
Alain Gras, Professeur
et de Sophie Poirot-Delpech, Maître de conférences,
Paris-I Panthéon Sorbonne

Septembre 2001

Remerciements

Ouf, c'est bouclé, on imprime tout ça et demain direction La Sorbonne pour rendre ce mémoire, mais avant : penser aux REMERCIEMENTS, eh oui, c'est un peu solitaire à la fin, ce genre d'exercice, l'œil rivé à son écran d'ordinateur, mais il y a eu tout plein de gens qui m'ont aidée toute l'année. Reprenons par ordre chronologique. "Top first" comme on dit à la Sorbonne, un big, very big merci à Nadine (Pilon) bien sûr qui a dit tiens oui, je finance, intéressant cette idée d'étude, allons-y. Merci Nadine pour ta confiance, témoignée tout au long de cette année. Ensuite, direction la fac : je souhaitais depuis longtemps travailler avec Sophie (Poirot-Delpech) et Alain (Gras) mais allaient-ils accepter une étudiante plus trop jeune, qui a fait de la psychologie cognitive dans son jeune temps, des Human Factors ensuite, et qui n'a jamais entendu parler de l'arraisonnement heideggerien ? Une rédemption est–elle possible ? oui ? Merci Sophie, pour ton accueil, ton soutien, j'ai beaucoup de chance de t'avoir pour professeur (tuteure ? directeur ? bref Tutoring Teacher, là on se comprend). Quant à Alain, bien que toujours jamais là car en congé sabbatique, il a été aussi souvent ici quand même grâce au mail électronique, ce formidable outil ! Tak !

Ensuite, il m'a fallu trouver des personnes qui acceptent une interview sur ce thème... un grand merci collectif pour tous les contrôleurs, superviseurs, safety managers, régulateurs, qui m'ont accueillie. Un merci particulier à Kamel, qui m'a ouvert le monde du trading.

Enfin, vient le temps de l'écriture, de la relecture, des corrections, de la réécriture, de la relecture, de ... merci à Cyril (Barriquault) pour nos discussions très utiles, ses encouragements, et à Denis (de la Burgade), pour sa relecture minutieuse, et ses éclaircissements très utiles pour la partie juridique.

Et, bien sûr, pour tous les encouragements que j'ai reçus, merci aux amis et famille qui m'entourent si chaleureusement, et à Laurent, merci pour TOUT.

Chapitre 1.
Introduction générale

Qu'est-ce cependant qu'une "dose raisonnable" de transparence et de secret ? La réponse est d'autant moins aisée à dégager que, eu égard à la charge symbolique qui s'attache aux concepts de transparence et de secret, leur invocation est fréquemment maniée comme une arme, moins pour dégager des compromis praticables, que pour faire pièce à des adversaires réels ou hypothétiques.

Rapport public du Conseil d'Etat. 1995. Etudes & documents, N° 47.

La transparence est une notion dans l'air du temps, et il suffit pour s'en convaincre de lire la presse de l'année écoulée[1]… Le terme est utilisé dans des domaines extrêmement divers : politique, économique, et même sportif. Quelques exemples récents : le Président Bouteflika propose deux semaines après le début des émeutes qui avaient ensanglanté la Kabylie, une commission d'enquête chargée de faire la lumière "*en toute liberté*" et "*en toute transparence*". Le Monde salue au passage le président "*qui a tenu parole en acceptant que le discours officiel soit ouvertement démenti et les autorités de l'Etat gravement mises en cause par les enquêteurs*".

La transparence n'est donc pas sans danger.

Christian Blanc, dans un article intitulé[2] "EDF, Service public, expansion et transparence", s'interroge, un brin sarcastique : "*la stratégie d'EDF relève-t-elle du secret d'Etat* ?" et rappelle : "*Il faut se souvenir qu'un des facteurs majeurs de la montée du sentiment antinucléaire, dans les années 1970, fut l'opacité entourant l'exposé des motifs*".

La transparence a quelque chose à voir avec la confiance.

La transparence a été maintes fois citée dans l'affaire des farines animales. Jean Puech, ancien ministre de l'agriculture, déclare qu'il regrette[3] "*de ne pas avoir été auditionné. Je me rappelle très bien, à l'époque, avoir pris tout de suite au sérieux ce dossier. D'autant que c'était la période de l'affaire du sang contaminé. J'ai organisé immédiatement la transparence, en publiant notamment des communiqués de presse à chaque abattage, qui n'étaient jamais repris dans les média*".

La transparence peut donc "*s'organiser*".

Le domaine financier n'est pas en reste : attribution des stock options dans l'entreprise, débat sur l'opportunité de publier les salaires des PDG les plus payés en France. Quant au bon vieux Tour de France, le voici lui aussi enfin converti : "*Le Tour de France du nouveau siècle promet la transparence*"[4] titre toujours le même journal, pourtant peu enclin aux envolées lyriques.

La transparence est à la mode.

Ces exemples concernent une revendication de transparence comme vertu démocratique. Le secret est souvent devenu, dans les différentes affaires mentionnées, synonyme de scandale : derrière la diversité des domaines dans lesquels la notion est employée se profile en commun le souci d'un accès à l'information, cette information étant considérée comme critique, essentielle du point de vue des personnes qui souhaitent y avoir accès, qu'il s'agisse de santé publique (le droit de savoir ce que l'on mange), ou de justice dans la répartition des richesses financières de l'entreprise. A un premier niveau, il existe des informations qui ne doivent pas m'être cachées (à moi, citoyen, salarié,…) : il s'agit concrètement par exemple de la visibilité d'un processus de décision par ceux qui sont extérieurs à ce processus, mais qui seront néanmoins touchés par les conséquences de ces décisions. Mais il existe aussi d'emblée dans ce terme un supplément de sens, une connotation positive[5] (la transparence évoque la pureté, c'est : "transparent comme de l'eau de roche") alors que le terme de visibilité, par exemple, qui renvoie à la même notion, sonne de façon bien plus prosaïque.

La transparence a une charge symbolique.

---

[1] Par exemple, en Août 2001, à l'aide d'une recherche Internet : on trouve 33 articles dont le titre comporte mot "transparence" sur les 3 derniers mois dans "Le Monde".
[2] Le Monde du 27/07/01
[3] Le Monde du 18/05/01
[4] Le Monde du 06/07/01.
[5] Helen Wallace fait remarquer qu'en Langue anglaise "Transparency" n'a pas de signification politique particulière ou de résonance, alors que d'autres termes tels que "accountability" ont un poids plus grand dans les débats sur la démocratie. (H. Wallace, Transparency and the legislative process of European Union, Actes du colloque organisé par le CEDORE (Nice) sur "La transparence dans l'Union européenne. Mythe ou principe juridique ?" 1999. L.G.D.J.

Dans ces différents exemples, on peut lire quelques caractéristiques de la transparence :

- ➔ C'est un processus vertical plutôt qu'horizontal. Ainsi, des citoyens réclament plus de transparence à leurs gouvernants, des salariés à leurs dirigeants. la transparence est rarement un processus qui se passe entre pairs, égaux.

- ➔ La transparence n'est normalement qu'un moyen, et pas un but en soi. Lorsque le gouvernement réclame à une association la transparence sur ses comptes et financements, c'est au nom d'une autre valeur : que les donateurs ne soient pas floués et que les dons qu'ils effectuent soient bien alloués à la cause qu'ils souhaitent défendre. Dans ce cas, l'information (les comptes) a du sens et la transparence des comptes n'est qu'un "moyen". Lorsque des salariés souhaitent que les attributions de salaires et primes soient effectuées de façon transparente, c'est au nom d'une certaine idée d'égalité au sein de l'entreprise. L'information dévoilée "fait sens" à l'aune de certaines valeurs.

Un autre versant de la notion concerne cette fois ci la transparence de l'individu vis-à-vis des autres, ou vis-à-vis d'un pouvoir central (par exemple, le fameux "Big Brother" d'Orwell), avec les questions liées à la vie privée, à l'intimité. Avec un paradoxe qui n'est peut être qu'apparent : d'un côté, inquiétude quant à des techniques qui sont de plus en plus "intrusives" (Internet, vidéo-surveillance), d'un autre côté, mise en place d'une forme de transparence par l'individu lui même avec une tendance contemporaine à l'exposition publique de soi, en littérature[6], mais aussi dans un jeu télévisé qui fit couler beaucoup d'encre. Le tout nourri de nombreux débats : là où l'académicien Bertrand Poirot-Delpech[7] regrette les "*fausses transparences*" de l'artiste, rend hommage à des amis perdus ("*l'honnêteté et le charme augmentent avec le refus de l'exhibition*") et cite Lacan ("*la vérité ne peut se dire toute*"), le sociologue Jean Paul Kauffman[8] ne constate rien moins qu'une forme de "*mutation anthropologique*" : c'est la place de l'intime qui est entrain de changer dans notre société. Il est "*désormais subordonné à l'extériorisation de soi qui devient le trait dominant des sociétés contemporaines*".

Dans le travail exposé ici, une approche anthropologique large qui s'interroge sur la transparence, la notion d'intimité, et la place des objets techniques dans la construction de cette transparence va se resserrer ensuite sur une approche plus proprement sociologique qui va étudier les enjeux de cette transparence dans une organisation comme la navigation aérienne.

On distinguera, le plus souvent possible, d'une part, ce qu'on peut appeler "*la transparence de l'organisation*", ou la transparence comme vertu politique, dans le premier sens exposé ci-dessus, et d'autre part, "*la transparence de l'individu*", le second versant des exemples exposés ci dessus. Cependant, dans une approche plus générique de la transparence, notamment sous l'angle philosophique, cette distinction n'a plus toujours sa pertinence. En outre, on parlera aussi *d'Auto Transparence* pour décrire le processus par lequel une organisation réfléchit sur son propre fonctionnement.

Le plan de ce document est le suivant :

Le chapitre 2 résume les visions philosophiques, politiques et juridiques de la transparence dans une approche critique.

Le chapitre 3 questionne le problème spécifique de la transparence dans un contexte d'organisation dit "*à hauts risques*".

---

[6] Bien sûr, dans le domaine littéraire, on se souvient de la déclaration de Rousseau dans ses Confessions : "Je voudrais pouvoir en quelque façon rendre mon âme transparente aux yeux du lecteur, et pour cela je cherche à la lui montrer sous tous les points de vue, à l'éclairer par tous les jours, à faire en sorte qu'il ne s'y passe pas un mouvement qu'il n'aperçoive, afin qu'il puisse juger par lui-même du principe qui les produit".

7 Fausses Transparences. B. Poirot-Delpech, Le Monde du 17/04/01

8 Voyeurisme ou Mutation Anthropologique ? J.P. Kaufmann. Le Monde du 10/05/01

Le chapitre 4 développe le rôle des nouveaux objets techniques vis-à-vis de la transparence.

Le chapitre 5 présente le cas particulier de l'organisation de contrôle du trafic aérien en Europe. Le cas d'un outil lié à la transparence (l'Automatic Safety Monitoring Tool) est aussi présenté.

Le chapitre 6 consiste en une étude comparative de cinq organisations de contrôle de trafic aérien quant aux problématiques de transparence qui ont été énoncées dans les chapitres précédents.

Le chapitre 7 présente la conclusion générale.

Chapitre 2.
Quelques angles d'approche de la notion de transparence

Le cabinet superbe et solitaire
Du secret de Titus est le dépositaire.

Bérénice, Racine.

2.1. Introduction

Dans ce chapitre, on se propose d'explorer la notion de transparence sous différents angles.
L'angle philosophique sera très modeste : si on peut faire un lien assez immédiat entre transparence et modernité, l'approfondissement de ce lien implique toute une réflexion sur l'héritage des Lumières et la naissance de la Modernité qui ne sera ici que très brièvement évoquée grâce aux réflexions de G. Vattimo. Le lien entre transparence et pouvoir sera davantage détaillé, et repris dans la partie consacrée aux débats. Les composantes politiques et juridiques seront ensuite présentées, ainsi que quelques notions complémentaires telles que le secret, la vie privée, la confiance ; enfin, la conclusion de ce chapitre permet d'ouvrir sur quelques débats qui trouveront leur résonance dans la réflexion menée dans l'organisation du contrôle aérien dans les chapitres suivants.

2.2. Un concept transversal

2.2.1. Petite philosophie de la transparence

Une valeur moderne

Dans le sens essentiellement politique qui nous intéresse, la transparence est une notion récente. Le terme apparaît dans les années 70, et connaît depuis une vogue qui semble trouver son apogée (du moins en France) ces dernières années, peut être même durant l'année écoulée.

Cette notion est quasiment toujours accolée à la Modernité. Est-ce un hasard si l'architecture contemporaine fait un large usage du verre, nous permettant souvent de "*voir le dedans ?*", de voir à travers les murs ? Il est certes indispensable que l'industrie ait d'abord été capable d'élaborer des verres d'une qualité exceptionnelle pour permettre son utilisation sur d'immenses surfaces, mais il est tout aussi vrai que la transparence permise par le verre est souvent soulignée comme emblématique de notre architecture contemporaine par ceux qui la font et ceux qui la critiquent, qu'ils l'aiment ou la détestent.

Dans "*La société Transparente*"[9], le philosophe italien Vattimo explore les rapports entre Modernité et Post Modernité. Son analyse part du lien entre Modernité et transparence dans le sens particulier d'une "*Auto transparence*". Il déclare : "*Les idéaux sociaux de la Modernité peuvent être décrits comme guidés par l'utopie d'une Auto transparence absolue*". Il existe donc d'emblée un lien entre transparence et vérité, transparence et raison. Le Positivisme de Comte peut d'ailleurs être compris en le rapprochant du programme Hégélien de réalisation de l'Esprit absolu, et l'auto-transparence complète de la Raison. Il s'agit, en fait, du cœur même du programme des Lumières : obtenir une "*auto conscience*" de l'humanité, notamment dans la sphère publique qui serait débarrassée du dogmatisme, des préjugés, de la superstition… Cet idéal, constate Vattimo, est d'ailleurs très présent dans les pensées d'auteurs tels qu'Habermas ou d'Apel car, dans les théories communicationnelles, c'est bien une "*transparence complète de la communication*" qui est visée. Il faut retenir que la notion d'objectivation est donc très liée au thème de la transparence.

Dans "Le Culte de l'Internet[10]", Philippe Breton analyse comment cet idéal d'auto-transparence est développé et porté par la rhétorique qui entoure Internet. Il analyse d'abord le glissement qui s'opère entre "information" et vérité" : l'information devient "*le but ultime à atteindre*". La transparence

[9] The Tranparent Society. Gianni Vattimo. The Jonh Hopkins University Press. Baltimore. 1992.
[10] Le culte de l'Internet : une menace pour le lien social ? Philippe Breton. La Découverte. 2000.

devient la traduction immédiate de ce culte de l'information[11]. Dans les discours des grands enthousiastes d'Internet stigmatisés par Breton, "*la société mondiale de l'information peut se définir comme un monde ainsi "transparent à lui même" qui ferait enfin reculer la violence et constituerait l'idéal ultime de la civilisation*".

En outre, pour Breton, si le culte de la transparence s'enracine dans le culte de l'information, il s'autonomise de plus en plus. Il devient fin et non moyen, pour reprendre les termes de notre introduction. La transparence tend alors dangereusement à s'ériger comme valeur en soi. Selon Breton, c'est exactement ce culte de la transparence qui est donné par l'expérience de la "maison de verre", une expérience menée dans l'Ohio[12]. Dans cette expérience, cinq amis montrent leur vie privée au monde des internautes, grâce à des "webcams" qui les filment en permanence et diffusent ces images sur le réseau. Breton note que la question de la finalité d'un tel projet n'est même pas *questionnée*, tant il est évident qu'il ne s'agit de rien d'autre que de la "*mise en œuvre, concrète, de l'idéal de transparence*", dès lors érigée en "*élément de foi*". Il semblerait que l'information montrée n'ait aucun sens, ce qui importerait c'est le processus de "*montrer*", la transparence mise en œuvre[13]. Il faut retenir de cette analyse de Breton que la transparence peut oublier le "*sens*" de l'information pour devenir une valeur en soi.

Un instrument de pouvoir

Une autre question, à la frontière de la philosophie et des sciences politiques, concerne la "mise en transparence" des individus par un pouvoir quelconque. Bentham reste célèbre pour son fameux "panopticon", dont il a défini l'architecture idéale sous la forme d'une tour entourée d'un anneau divisé en cellules. Les ouvertures des cellules, vers la tour et vers l'extérieur de l'anneau permettent à un surveillant qui se trouverait dans la tour de voir toutes les cellules et leurs occupants dont les silhouettes se détachent en contre-jour. Mais on ne retient souvent de ce dispositif architectural que la description très critique qu'en donne M. Foucault dans "Surveiller et punir". Or, il importe de replacer ce projet élaboré par Bentham dans le contexte de la philosophie utilitariste : "*maximisation du plus grand bonheur pour le plus grand nombre*". Dans l'utilitarisme, il y a un "saut" comme l'explique Laval[14], du principe individuel du plaisir à un principe d'utilité posé comme socle de d'organisation politique. Bentham est aussi un réformateur, un esprit progressiste : si le principe d'utilité n'a pas été reconnu comme le principe de base de la construction politique et juridique, c'est, considère-t-il, que "*les intérêts funestes de la minorité dirigeante l'ont emporté jusqu'à présent sur le bonheur du plus grand nombre des dirigés*". Le panopticon n'est donc, pour Bentham, avant tout, qu'un des outils au service de la construction d'une société "meilleure" [15] Qu'une telle société contienne en germe les fondements d'une forme de dictature par la régulation des conduites qu'elle instille, ou qu'elle soit le fondement d'une démocratie est une autre question qui reste ouverte[16].

Foucault, dans "Surveiller et Punir", propose une description du panopticon articulée à la notion de pouvoir. Il souligne d'abord, dans le panoptique, le mécanisme de contrôle et de "mise en visibilité" des individus. Ainsi, chaque occupant d'une cellule (un fou, un malade, un ouvrier, un écolier) précise Foucault, qui décrit bien un dispositif disciplinaire plus qu'une simple architecture de prison, n'échappe plus à une visibilité de tous les instants. Il s'agit bien du principe architectural d'une forme de transparence, décrit ainsi par Foucault : "*dans la fameuse cage transparente et circulaire, avec sa haute tour, puissante et savante…*", qui est en même temps "*le diagramme d'un mécanisme de pouvoir ramené à sa forme idéale*".

---

[11] Dans ses recherches précédentes, Breton avait analysé en quoi le paradigme informationnel est caractéristique de la Modernité, et comment ce paradigme avait remplacé d'autres pôles de la Parole tels que l'*argumentatif* et le *sensible*.

[12] Depuis, il semble que ce type d'expérience existe aussi à la Télévision.

[13] Toutefois ce phénomène de mise en transparence de vies privées offre d'autres possibilités d'interprétations. Sophie Poirot-Delpech (communication personnelle) remarque qu'il ne s'agit peut être là que d'une manifestation de la marginalité qui trouve dans la technique internet une nouvelle modalité d'expression.

[14] Christian Laval. Jeremy Bentham, Le pouvoir des fictions. PUF. 1994.

[15] Bentham préconisa la réduction du recours à la sanction pénale, lutta pour le vote des femmes, l'accès à la justice des pauvres, etc. Utilitariste jusqu'au bout, selon ses dernières volontés, son cadavre est disséqué publiquement pour servir la science. (Laval, op.cit.)

[16] Actualité de la pensée juridique de Jeremy Bentham. Facultés universitaires de Saint Louis, 1987. Philippe Gérard, F. Ost, M. Van de Kerchove.

Forme idéale au sens où l'entend Foucault, c'est-à-dire, semble-t-il, un pouvoir en quelque sorte automatique et désincarné, intégré si intimement et si subtilement dans chaque conscience qu'il ne reste plus de conscience d'un pouvoir subi, extérieur. Le pouvoir est ici à la fois "visible et invérifiable" : visible parce que le détenu voit la tour dont il est épié, et invérifiable car le détenu ne sait jamais s'il est regardé. De plus, le principe classique d'une réciproque "voir-être vu" est dissocié. En effet, le détenu est toujours vu, et la personne dans la tour jamais vue, par le jeu subtil des contre jours. Ce qui induit chez le détenu, comme l'explique Foucault, "*un état conscient et permanent de visibilité qui assure le fonctionnement automatique du pouvoir*".

Enfin, dernier aspect essentiel de cette modalité du pouvoir explorée par Foucault, le pouvoir est *désindividualisé* : c'est le dispositif qui met en place ce pouvoir, et non un individu en particulier. Chez Foucault, la transparence est un concept intrinsèquement lié au pouvoir, et elle est transparence du "*dominé*" pour le "*dominant*", une caractéristique essentielle du Panopticon est bien le caractère radicalement unilatéral de cette mise en visibilité.

2.2.2. L'approche politique

Un principe de régulation

La notion de transparence est au cœur de l'analyse politique des institutions : elle y est vue avant tout comme un principe de régulation politique ("*la transparence joue le rôle d'un mythe de référence de l'ensemble de systèmes de pouvoir*" souligne le Professeur Rideau[17]), et on y souligne souvent la difficulté à lui donner une définition précise. Ceci ne va pas sans rappeler l'emploi pléthorique du terme dans la presse que nous avons souligné dans l'introduction. La transparence est même qualifiée de "*notion molle*" par Lequesne[18], rejoignant dans cette catégorie les termes de "subsidiarité" ou d' "évaluation". Beaucoup d'auteurs voient dans l'absence de définition précise une faiblesse, voir un effet de mode un peu agaçant (cf. les critiques présentées dans la partie "Débats" ci-dessous) mais Lequesne défend au contraire que "*cette polysémie permet à chaque citoyen d'y trouver des connotations positives*". De plus, cette plasticité, souligne-t-il, permet une application au cas par cas : or, les citoyens des démocraties contemporaines semblent apprécier que la règle de Droit fasse appel à une mise en oeuvre différenciée.

Les politologues articulent souvent dans leurs réflexions les deux problématiques de la transparence qui ont été identifiées dans l'introduction : d'une part, la transparence des "gouvernants" aux "gouvernés", (par exemple : du pouvoir politique aux citoyens, de l'institution au sujet) ; d'autre part la transparence de l'individu envers un pouvoir, quel qu'il soit (avec les problèmes de vie privée, d'intrusion grâce aux nouvelles technologies, *etc.*). Ce que nous avons appelé : la *transparence de l'organisation* et la *transparence de l'individu*.

En ce qui concerne la transparence du pouvoir aux gouvernés, le lien entre transparence et démocratie est assez immédiat, et très convenu[19]. Transparence et autocratie ne font pas bon ménage : la formule de Napoléon, affirmant qu'une constitution devait être "*courte et obscure*", symbolise l'opacité du pouvoir autoritaire, comme le rappelle Rideau[20].

Un pas de plus est franchi avec les régimes totalitaires, dans lesquels le domaine public est opaque aux gouvernés, et la vie privée devient transparente pour le pouvoir central : c'est le "*Big Brother is watching you*" d'Orwell.

---

[17] Cité par Noelle Lenoir. Conclusion. Actes du colloque organisé par le CEDORE (Nice) sur "*La transparence dans l'Union européenne. Mythe ou principe juridique ?*" L.G.D.J. 1999.

[18] *La transparence, vice ou vertu des démocraties*, Christian Lequesne. Actes du colloque organisé par le CEDORE (Nice) sur "La transparence dans l'Union européenne. Mythe ou principe juridique ?" 1999. "L.G.D.J."

[19] "(La démocratie) ne peut s'accommoder de l'ombre ou de la pénombre. Elle ne peut fonctionner à huis clos. Entre "professionnels" de la politique. Loin de ces gêneurs que seraient les lecteurs et les électeurs" (R.-G. SCHWARTZENBERG, "A ciel ouvert", *Le Monde* 10 novembre 1979, p. 5). Cité par Denis de La Burgade, *La vie privée des hommes politiques*, Thèse de doctorat, Paris I, 2000.

[20] Joël Rideau. *Jeux d'ombre et de lumière en Europe*. Actes du colloque organisé par le CEDORE (Nice) sur "La transparence dans l'Union européenne. Mythe ou principe juridique ?" L.G.D.J. 1999.

Dans les démocraties contemporaines, la notion de transparence se développe dans les années 70. Il s'agit d'abord d'opposer à l'opacité administrative, "*la figure antithétique de la transparence conçue comme pure positivité*", selon la formule de Jacques Chevalier[21]. Depuis les années 80, la transparence devient une valeur en hausse, et touche de nouveaux domaines, notamment financier.

La construction européenne développe le thème d'une meilleure transparence des décisions communautaires lors de sa campagne référendaire. C'est à partir du Traité de Maastricht[22] que la transparence a été intégrée dans les objectifs politiques de l'Europe dans la déclaration relative au droit d'accès à l'information annexée à l'acte final, dans laquelle les Etats proclament que "l*a transparence du processus décisionnel renforce le caractère démocratique des institutions ainsi que la confiance du public envers l'administration*". Ce processus est renforcé par le Traité d'Amsterdam, qui au-delà de la transparence administrative, entend renforcer la lisibilité du droit communautaire. L'objectif visé est bien de rapprocher l'Europe du citoyen.

Une réponse à l'imprévisible ?

Transparence, lisibilité et confiance sont donc des notions liées. Jean-Denis Bredin[23] a souligné la transparence comme réponse, une compensation à l'imprévisibilité. C'est parce que le futur de notre époque se caractérise par l'imprévisible, que la transparence est nécessaire, car elle est une composante, une condition de la maîtrise du présent, affirme-t-il. Il nous semble toutefois que la notion de transparence prend une résonance nouvelle, beaucoup plus dramatique, avec les problèmes du risque sanitaire apparus avec l'affaire du sang contaminé, et se développant avec les affaires d'ESB, d'OGM,… La notion de transparence glisse alors vers un sens nouveau dans lequel on ajoute à l'imprévisibilité du monde, *l'imprévisibilité des risques*.

Chez Hannah Arendt[24], la question de l'imprévisible est également posée dans "*La condition de l'homme moderne*". La source de l'imprévisibilité chez Arendt n'est pas seulement, comme chez Bredin, une caractéristique de notre époque. Elle est liée à la faiblesse humaine, à sa versatilité (l'homme ne peut garantir qui il sera demain) et à "*l'impossibilité de prédire les conséquences d'un acte dans un monde d'égaux où tous ont la même faculté d'agir*". Mais Arendt considère la promesse comme réponse à cette imprévisibilité, et considère cette réponse comme une caractéristique essentielle de notre condition moderne. "*Le pouvoir de stabilisation propre à la faculté de faire des promesses a été reconnu dans toute notre tradition*". La métaphore de la transparence n'est pourtant pas loin, puisque "*la fonction de la promesse est de dominer cette double obscurité des affaires humaines*". On pourrait penser que pour l'*imprévisible* dont parlait Hannah Arendt à son époque, la promesse était un mécanisme régulateur suffisant, en y adjoignant le Pardon, qu'Arendt considère comme l'autre grand mécanisme régulateur de la société dans laquelle elle vivait. Mais cet imprévisible prend dans notre société une dimension nouvelle[25], dès lors la réponse serait la transparence totale, qui seule permettrait d'apporter une maîtrise suffisante. On verra dans le chapitre suivant que la réponse n'est pas non plus si simple.

Le Public de plus en plus public, le Privé de plus en plus privé ?

Si on considère maintenant les deux aspects de la transparence, on souligne souvent un double mouvement qui montre que ces deux problématiques ne peuvent jamais être étudiées de façon totalement séparées. Au début du siècle, le sociologue Simmel[26] avait constaté : "*il semble que plus la civilisation se spécialise, plus les affaires de la collectivité deviennent publiques, et plus celles des individus deviennent secrètes*".

---

[21] J. Chevallier : *le mythe de la transparence administrative*, CURAPP, n° 679. 1988.
[22] Ce qui s'est fait essentiellement sous la pression de pays du Nord de l'Europe (L'opaque transparence de l'Union Européenne. Ingrid Carlberg. Le Monde Diplomatique. Juin 1997).
[23] Jean Denis Bredin. *Secret, Transparence et démocratie*. POUVOIRS. N°97 Avril 2001.
[24] Hannah Arendt. La condition de l'homme moderne. AGORA, Calmann Levy. 1983.
[25] Jonas considère que cet imprévisible et de cette nouvelle dimension du risque exige une refonte de l'Ethique (Hans Jonas, le principe Responsabilité. Champs Flammarion. 1995).
[26] Simmel, Secret et société secrète. Circé. Poche. 2000. (Première édition : 1908).

La science politique actuelle aurait plutôt tendance à considérer que ce mouvement est loin d'être acquis, parfois même fort malmené, avec de nouveaux modes d'intrusion liés aux techniques. Un siècle après Simmel, Belorgey[27], par exemple, formule ce double mouvement comme un enjeu que les démocraties actuelles devraient atteindre à travers leurs lois, plutôt que comme un constat : "*assurer plus de transparence à ce qui est longtemps resté secret : les actes des pouvoirs, et plus de secret à ce que les pouvoirs ont durablement souhaité, et souvent réussi à scruter : la vie privée*".

2.2.3. L'approche juridique

Si, pour la science politique, la transparence peut être qualifiée de "*notion molle*", une sorte de valeur ou de vertu difficile à rendre opératoire, les juristes, quant à eux opposeront une vision, plus opérationnelle, dans laquelle la transparence est toujours transparence *de quelque chose*. Dès lors, elle s'ancre dans des lois sur la transparence, qui vont déterminer le caractère de ce qui est visible et les personnes qui vont accéder à l'information.

Des différences nationales

Les différences entre les grandes démocraties occidentales sont encore très importantes à ce sujet. Lassalle[28] considère la transparence comme une des valeurs centrales avancées par la démocratie américaine, et montre comment cet objectif est atteint par des moyens importants d'investigation et une multiplication de procédures : ce "fact finding" trouve son corollaire dans l' "exposure", (la publicité) qui fait l'objet du Freedom Of Information Act. (FOIA). La transparence y est conçue comme "*la recherche obstinée de la réalité des faits que les intérêts collectifs ou individuels tendent constamment à voiler*". Le Freedom of Information Act a été promulgué en 1966 et amendé en 1974. Le président Johnson, le jour de sa promulgation, soulignait le lien entre cette loi et les principes fondamentaux de la Démocratie américaine, et ajoutait "*une démocratie ne peut correctement fonctionner que lorsque le peuple dispose de toutes les informations compatibles avec la sécurité de l'état*". Il faut noter comme on l'a déjà souligné ailleurs que la transparence trouve toujours sa limite. S'agissant du FOIA, Lassalle considère que "*la transparence sert de contre pouvoir*", et montre que son champ d'application est particulièrement étendu[29], il n'en souligne pas moins les limites. Trois exceptions particulièrement importantes concernent les nécessités de la défense nationale et de la diplomatie, la protection de la vie privée, et le caractère confidentiel de certaines informations économiques ou financières. Aux Etats Unis, c'est le juge qui se prononce, en définitive, sur le caractère communicable ou non, d'une information. Des législations d'inspiration comparable à celle du FOIA existent aussi dans les pays d'Europe du Nord. La Suède, notamment, est un pays perçu comme un modèle en matière de transparence administrative.[30] Résolument pionnière puisque les lois sur la transparence administrative datent de 1766, avec l'arrivée au pouvoir des *Bonnets*[31] contre le parti des *Chapeaux* (!).

On oppose assez classiquement les pays du Nord de l'Europe et leur transparence et les pays du Sud, et leurs secrets, ou leur opacité… Le lien avec la religion est souvent évoqué : culture méridionale catholique contre protestantisme pour les pays Anglo-saxons. La France est souvent épinglée pour l'étendue des pouvoirs de secrets[32] (secret d'état en matière de politique étrangère et de défense, et

---

[27] Jean Michel Belorgey, L'état entre Transparence et Secret. POUVOIRS. N°97. Avril 2001.

[28] Lassalle. *La Démocratie américaine*. Colin, 1991.

[29] Par exemple, Scott Sagan, dont on citera plus loin le livre (*The limits of Safety*) sur les incidents liés aux armes nucléaires aux USA s'est servi du FOIA pour accéder aux données.

[30] Lequesne, mentionne qu'une enquête réalisée en Suède au début des années 80 a montré que les demandes de consultation émanant des citoyens sont en fait rares. Les utilisateurs les plus nombreux du droit d'accès sont en fait les journalistes suivis de près par les entreprises commerciales. Des enquêtes dans d'autres pays, propose t-il, sur l'utilisation du droit d'accès à l'information permettraient peut être de montrer que la transparence est un "mode de contrôle démocratique médiatisé", indirect, ce qui est caractéristique des démocraties contemporaines. Il semble, en revanche, que les citoyens américains accèdent plus volontiers directement à ces informations. *L'état entre transparence et Secret*. POUVOIRS. N°97. Avril 2001.

[31] *L'opaque transparence de l'Union Européenne*. Ingrid Carlberg. Le Monde Diplomatique. Juin 1997.

[32] Ainsi, Saul compare les "répertoires culturels" de la France et des USA, en s'appuyant sur les travaux de Ezrahi. Alors que la tradition française implique que les décisions de l'état soient prises "derrière des portes closes", les citoyens américains sont plus habitués à avoir accès au processus de prise de décision du gouvernement. "*As long as state officials agree on decisions, and as long as those decisions appear to be in the public's best interest, French citizens do not expect to be able to look at the decision-making process itself. Conversely, American citizens expect that they will have access to state decision-making processes, and that those processes will be visible (through such mechanisms as the Freedom of Information Act, the Federal*

secret administratif, sans parler du secret des archives publiques[33])… On parle souvent *d'opacité à la française* [34], Michel Crozier en a fait une caractéristique du fonctionnement étatique français.

La France en progrès

La transparence administrative en France résulte, à la fin des années soixante-dix, d'une série de textes législatifs spécifiques et autonomes mais dont la communauté d'inspiration est frappante en ce qu'ils consacrent peu ou prou l'existence d'un droit à l'information[35]. Il faut noter que ce n'est qu'a posteriori, que les politologues ont conféré à ces différentes lois le statut de "lois sur la transparence".

Le secret de la Défense nationale, avait été qualifié d' "angle mort de la transparence" par le rapport du conseil d'état en 1995. "*Le doute entoure aujourd'hui l'utilisation du secret de la défense, qui est parfois perçue comme abusive…".* Le texte de la loi du 8 Juillet 1998 portant création d'une commission consultative du secret de la défense nationale, marque un progrès sur la classification des documents administratifs, en instaurant une commission indépendante, chargée de décider si un juge a le droit ou non de prendre connaissance d'un document classifié. Une commission indépendante est donc chargée désormais de vérifier que le secret est opposé à bon escient. Depuis cette création, le gouvernement semble s'être donné pour ligne de conduite de suivre le sens de l' avis émis : il est vrai que la simple publication d'avis lui confère une autorité forte.

Le secret des archives publiques a été récemment questionné, souvent à l'occasion d'affaires ou de procès : par exemple, le procès de Maurice Papon, pour lequel les autorités politiques ont accepté de dévoiler certaines archives. Néanmoins ces avancées sont encore timides, si on compare le pouvoir des juges dans d'autres démocraties (britannique, américaine, espagnole, allemande…), qui sont autorisés à examiner les documents afin de décider du bien fondé de leur caractère secret. Les procédures sont légèrement différentes[36], mais il s'agit toujours d'opérer cet arbitrage entre l'intérêt public, argument classique du gouvernement, et la justice.

Dans certains cas, la solution préconisée est un sas entre transparence et secret. Ainsi le conseil d'état a préconisé la mise en place d'autorités administratives qui relèvent de l'Etat tout en étant indépendantes. C'est le cas, par exemple, de la CNIL et de la CADA. On parle de "magistrature du secret". Dans le cas de la transparence financière de la vie politique, une commission composée des plus hauts fonctionnaires et magistrats de l'Etat opèrent un contrôle du patrimoine des hommes politiques les plus influents afin d'éviter l'enrichissement personnel dans l'exercice du pouvoir. Ce contrôle reste a priori secret, en revanche en cas de variation anormale du patrimoine, la commission saisit le parquet, qui fait une enquête pénale. Il s'agit donc d'un cas de transparence sans "*publicisation*", dans laquelle Denis de la Burgade[37] distingue une *transparence interne* (vers la commission) et une *transparence externe* (vers le citoyen).

Register, Congressional hearings, etc.*)".* Saul fait l'hypothèse que cette opacité des processus de décision a joué un rôle important dans l'ampleur du drame du sang contaminé en France. *The Transparency of Blood, The construction of risk and safety during and after the AIDS blood scandal in France and the US*, Jessie E. Saul. Workshop on Social Construction of Risk and Safety, Villa Fridhem, Kolmården, Sweden, March 15-17, 2000

[33] La loi du 3 Janvier 1979 interdit d'accéder aux archives politiques tant que les protagonistes sont encore vivants.

[34] *Opacité à la française, cet archaïque secret d'Etat,* Joseph K. (haut fonctionnaire). Le Monde Diplomatique, Juillet 2000.

[35] Ce sont les lois "fondatrices" du 6 janvier 1978 relatives à l'informatique, aux fichiers et aux libertés, du 17 juillet 1978 améliorant les relations entre l'administration et les administrés et relative notamment à l'accès aux documents administratifs, du 3 janvier 1979 sur les archives et du 11 juillet 1979 sur la motivation des actes administratifs.

[36] Pour des exemples récents voir l'article de Joseph K. cité ci dessus.

[37] "*Jusqu'à présent, le dispositif législatif et réglementaire qui s'efforce de résoudre la "contradiction importante entre la volonté de permettre au citoyen de s'assurer que ses représentants n'abusent pas de leurs fonctions pour accroître leur fortune personnelle et la nécessité d'assurer le respect de la vie privée des personnes soumises à l'obligation de déclaration patrimoniale", privilégie la transparence "interne" aux détriments de la transparence "externe" faisant parfois naître dans l'opinion publique un sentiment de dépossession".* Denis de La Burgade, *La vie privée des hommes politiques*, Thèse de doctorat, Paris I, 2000

2.3. Une réalité multiple

2.3.1. Le secret ou la face noble de l'opacité

A l'opposé de la transparence, on trouve bien sur l'opacité, mais aussi, le secret, ("*la face noble de l'opacité*" comme l'appelle joliment Bredin). Si les visions politiques des relations gouvernants/gouvernés insistent sur la nécessité de la transparence dans une démocratie, certains sociologues s'intéressent plus au secret comme forme de lien social dans un collectif.

L'étude de Simmel "*Secret et société secrètes*" est peut être une des premières tentatives proprement sociologique de développer la notion de secret, en l'analysant en tant que tel et non seulement en négatif par rapport à ce qui est montré. En s'attachant à analyser que le sens que prend le secret dans toute relation entre les humains, il permet d'élaborer une vision plus positive du secret. "*La large négativité éthique du secret ne doit pas nous induire en erreur sur ce point : car c'est une forme sociologique universelle, qui recouvre de façon tout à fait neutre la valeur de ses contenus*".

Pour Simmel, dans toute société, il y a du visible et du caché, et il va jusqu'à formuler l'hypothèse d'un "*quantum de secret*" dans toutes les sociétés, qui ne ferait que se déplacer sur des contenus différents mais qui resterait constant. "*La coexistence des hommes, dans des circonstances par ailleurs égales, aurait besoin d'une certaine part de secret, celui-ci changeant seulement d'objet, abandonnant ceci pour s'emparer de cela, et dans cet échange son quantum resterait inchangé*".

Pour audacieuse et invérifiable qu'elle soit, cette hypothèse n'en est pas moins stimulante, puisqu'elle redonne une place positive au secret dans un groupe social. En effet, on l'a vu à maintes reprises, dans les sciences politiques, le secret est souvent abordé comme secret gardé par un groupe vis-à-vis d'un autre groupe (classiquement, le secret d'un pouvoir vis-à-vis de ceux qu'il gouverne), et non pas comme lien au sein d'un collectif. Avec Simmel, le secret est aussi une forme de l'*être ensemble*. Dans son analyse des sociétés secrètes, il analyse comment "*le secret détermine les formes d'existence de tous ceux qui le détiennent ensemble*".

2.3.2. La vie privée : une notion récente, de nouvelles questions

La vie privée est une notion relativement récente. Hannah Arendt explique qu'au sens grec, le terme de vie privée s'appuie sur le caractère *privatif* : la vie privée est *privée de* (de la vie de la cité, de la vie politique, bref, de ce qui est plus intéressant que la vie domestique). La notion d'espace privé séparé d'une partie où l'on reçoit par exemple n'apparaît qu'à la renaissance. Ce n'est qu'au 18 ème siècle que la vie privée apparaît comme une valeur en soi. Elle devient alors constitutive de l'individu moderne, du sujet.

Dans le Droit, cette notion n'apparaît que récemment. La convention européenne des droits de l'homme détermine le droit à la vie privée, ce qui passera dans le droit français en 1970 (Art. 9 du code civil).

Cependant, la notion de vie privée est très contingente. La frontière entre ce qui révèle de la vie privée et ce qui doit être public est historiquement mouvante. C'est le cas, par exemple, du patrimoine. Il a longtemps été considéré, en France, comme secret, privé. Voici quelques années, un journal a publié le patrimoine du PDG de la société PSA, Jacques Calvet. Le juge, saisi par Jacques Calvet, considéra comme légitime la publication du patrimoine de Jean Calvet car PSA était en train de supprimer des emplois. A partir de cet épisode, la jurisprudence tergiversa sur le caractère privé ou non du patrimoine.

Enfin, cette notion est requestionnée, comme on l'a vu dans l'introduction, par de nouvelles pratiques artistiques d'exposition de soi : on peut les considérer comme marginales, ou y voir une "mutation anthropologique" comme le sociologue Jean-Paul Kauffman. Mais il s'agit bien d'une vie privée, d'un intime, montré volontairement par un individu qui choisit (et revendique) ce qu'il expose. En

revanche, chaque nouvelle technique permettant une forme d'intrusion dans la vie privée (on en verra de nombreux exemples dans le chapitre suivant) soulève de nombreux débats. La notion d'intime et de vie privée a donc toujours du sens pour les individus. On peut aussi en avoir pour preuve la nombreuse jurisprudence sur la surveillance des salariés, qui revendiquent toujours le droit à une forme d'intimité au travail, en souhaitant par exemple que leur employeur ne lise pas leur courrier électronique.

2.3.3. La confiance

Là aussi, la relation entre transparence et confiance paraît aller de soi. Le Député Jean Yves Le Déaut[38], à propos d'EDF, parle d'*une plus grande transparence… afin de restaurer la confiance*. Oui, mais quel degré de transparence ? Quel est le supplément de transparence à apporter pour restaurer la confiance ? Et ceci suffit-il ? Lorsque Claude Birraux[39] déclare, : "*la transparence doit être totale, quitte à perdre toute crédibilité*", veut-il dire aussi "*toute confiance*" ?

Simmel[40] énonce très clairement les rapports entre confiance et transparence : "*la confiance est aussi un état intermédiaire entre le savoir et le non savoir. Celui qui sait tout n'a pas besoin de faire confiance, celui qui ne sait rien ne peut raisonnablement même pas faire confiance*". En outre, il écrit : "*L'objectivation de la culture a établi des distinctions très nettes entre les différents quanta de savoir et de non savoir nécessaires à la confiance*". Il donne ainsi des exemples (de chercheur, commerçant, chef de parti politique) et il ajoute qu'ils "*savent ce qu'il est nécessaire de savoir pour la relation qu'ils veulent établir*".

Si cela était sans doute assez vrai dans le monde décrit par Simmel, au début du XXème siècle, il nous semble que la question se pose avec une acuité nouvelle, dans la société actuelle. Comme on l'a dit plus haut, le monde est maintenant plus "imprévisible", plus complexe… Si on reprend de nouveau l'exemple des risques sanitaires récemment soulevés, il est douteux que la culture ait peu à peu défini des "*quanta de savoir et de non savoir nécessaires à la confiance*". Dans ce cas, la transparence *totale*, permet justement de se passer de la confiance, comme le dit Simmel en d'autres termes. Mais lorsqu'on parle d'un système complexe, (le Nucléaire, le contrôle de trafic aérien) ou d'un problème complexe (l'ESB), quel contenu opératoire peut bien avoir la *transparence totale* qui fasse sens pour un citoyen ? Dans le chapitre consacré à l'application de la notion de transparence à une organisation à risques, le contrôle du trafic aérien, on verra que cette question peut se poser de façon très concrète, et que la notion de confiance ne peut être éliminée si vite.

2.4. Quelques débats

2.4.1. Une "frénésie de transparence"?

Si, comme nous l'avons vu en introduction, la notion de transparence se développe comme valeur, ce n'est pas sans susciter la méfiance ou même l'inquiétude face à ces excès.

Un premier type de critique est d'ordre pragmatique : la transparence doit rester raisonnable, parce qu'elle est en concurrence avec d'autres objectifs. Denis Kessler[41] analyse l'émergence du principe de transparence dans le domaine de l'entreprise : le développement des technologies de communication, l'évolution des organisations des entreprises, l'évolution d'un actionnariat désormais sur fonds propres, et bien sûr l'évolution du Droit avec ses nombreuses lois sur la transparence financière accompagnent le développement d'une plus grande transparence. Mais il existe bien sûr des intérêts contradictoires, par exemple ceux qui concernent la concurrence. L'obligation d'information aux salariés peut entrer en concurrence avec celle à laquelle elle est tenue vis-à-vis du marché : dans un

[38] Le Monde du 8 Juillet 1998.
[39] *Le contrôle de la sûreté et de la sécurité des installations nucléaires*. Claude Birraux. Economica, 1992.
[40] Secret et société secrète. Circé. Poche. 2000. (Première édition : 1908).
[41] Denis Kessler. *L'entreprise entre transparence et Secret*. POUVOIRS, n°97. avril 2001, Seuil

cas, délit d'entrave, dans l'autre, délit d'initié. Dans une veine plus polémique, Alain Etchegoyen ne mâche pas ses mots : "*Soyons honnêtes, aucune entreprise ne peut être transparente quand elle a une stratégie !*".

De façon plus fondamentale et plus politique, en s'interrogeant sur le sens profond de la vogue de cette notion, d'autres s'alarment de cette "*frénésie de transparence*" comme la nomme le juriste Guy Carcassonne[42], qui considère que les institutions sont désormais jugées par leur degré de transparence, au détriment d'autres critères. C'est bien sûr l'excès qui est ici stigmatisé ("*nous n'avons renoncé à un secret maniaque que pour glisser dans une névrose de transparence*"), et la focalisation sur cette valeur qui devient dogme, confondant fins et moyens. Or, rappelle Carcassonne, la transparence, au lieu d'être une fin en soi, est classiquement "*un moyen, comme d'autres et parmi d'autres, d'atteindre les finalités supérieures que porte en elle l'idée démocratique*" , et "*son utilité, comme sa légitimité, se mesurent à l'aune des objectifs qu'elle sert*". Devenue dogme, elle se rapprocherait plus du totalitarisme que de la démocratie.

Quant à Bredin[43], il s'inquiète : "*la transparence ne deviendrait-elle la vertu suprême, voir l'ultime vertu d'une société qui n'en porterait plus d'autre ?*".

2.4.2. Transparence et pouvoir

Le lien entre transparence et pouvoir est présent, du moins implicitement, dans toutes les réflexions politiques et juridiques. De façon plus fondamentale, "Le Prince" de Machiavel expose le jeu de la manipulation dans le gouvernement des hommes, et l'opacité des desseins du Prince comme un garant de son pouvoir sur les hommes. Cependant, Anne Torrès, expliquant sa mise en scène du Prince, souligne ce qu'elle considère comme le paradoxe majeur de Machiavel. "*Machiavel explique qu'il est impossible de gouverner dans la transparence. Mais en même temps, il rend transparente la non-transparence du pouvoir*"[44]. *Car éclairer, pour un Prince les méandres du pouvoir, c'est en analyser les mécanismes, et par là même, c'est aussi en "donner les clefs au peuple*".

Dans le domaine de l'analyse stratégique, en sociologie organisationnelle, Crozier et Friedberg[45], définissent le pouvoir comme "*l'échange déséquilibré de possibilités d'actions entre un ensemble d'acteurs individuels et/ou collectifs*". Le pouvoir n'est pas considéré comme un attribut, il ne se possède pas, il s'exerce dans une relation concrète. Le pouvoir dépend notamment de la liberté ou de la zone d'autonomie dont l'acteur dispose dans ses transactions avec les autres et qui détermine la prévisibilité de son comportement. Or, pour l'analyse stratégique, tout acteur au sein d'une organisation dispose d'une *marge d'opacité*, qui est toujours définie par une situation concrète. Enfin, il n'y a pas de pouvoir sans négociation.

2.4.3. La transparence opaque : les avatars d'une "fausse" transparence

On retrouve de façon récurrente, dans les analyses critiques de la notion de transparence, l'idée d'une "*transparence opaque*". Derrière cet oxymoron un peu facile, il existe une vraie question sur l'opposition entre transparence et interprétation, et sur le statut de l'acteur social dans sa volonté (sa prétention peut être) à "révéler" la vérité.

Cette question est abordée concrètement par le sociologue Shmuel Trigano[46] dans une analyse de deux types de discours actuels sur la Shoah : la thèse qui défend le caractère unique, la singularité de la Shoah, comme "*énigme transcendante et sacrée*" , et la thèse opposée, qui condamne "*l'excès de mémoire*", et "*l'occultation des autres souffrances*".

---

[42] Guy Carcassonne. *Le trouble de la transparence*. POUVOIRS, n°97. avril 2001, Seuil.
[43] Jean Denis Bredin. *Secret, transparence et démocratie*. POUVOIRS, n°97. avril 2001, Seuil.
[44] Le magazine Littéraire. N°397. Avril 2001. Interview de Anne Torres. *Le Prince* de Machiavel. Théâtre des Amandiers, Nanterre.
[45] Crozier Michel et Friedberg Erhard. *L'acteur et le système*. Points, Seuil, 1979.
[46] Shmuel Trigano. *La transparence opaque. La Shoah entre "abus de mémoire" et "idéologie moderne".* POUVOIRS, n°97. Avril 2001, Seuil.

Dans les deux cas, il s'agit bien de comprendre, de rendre transparent, ce qui était opaque, ou en d'autres termes aussi, de prétendre détenir la clef de l'explication d'un phénomène (la Shoah) incompréhensible. Or, pour Trigano, "*il n'y a de transparence que dans l'idéologie, qui a la prétention de tout expliquer, elle n'existe pas naturellement, car la réalité est naturellement opaque, non immédiatement compréhensible, et nécessitant une interprétation*". Pour Trigano, cette opposition peut être considérée comme un cas d'école de la sociologie de la connaissance de Mannheim : chaque acteur social ne voit qu'une partie de la réalité et les idéologies, dans ce cadre, sont des points de vue différents d une même réalité. De plus, ajoute Trigano en faisant référence cette fois-ci à Louis Dumont, chaque idéologie prétend rendre transparent un phénomène alors que l'homme moderne est acculé a une opacité congénitale car il est impossible de penser pour l'homme moderne autrement que dans les cadres de la modernité : en se confrontant à la Shoah, la conscience moderne des deux idéologies "en lice" se confronte à son *impensé.*

Ce qui est intéressant pour notre propos ici, c'est la réflexion sur le caractère idéologique de la transparence (idéologique est pris ici au sens sociologique de "*système de représentations attaché à une position dans la réalité sociale*"). A l'opposé de la transparence révélant la vérité, on aurait l'idée que l'explication d'un phénomène est toujours dépendant de la position de l'acteur social, et on introduirait la notion d'interprétation, et le sens de l'information dévoilée.

2.4.4. Transparence et sens

Le concept de "sensemaking" proposé par Weick[47], que l'on pourrait traduire par "construction de sens" est intéressant pour explorer les rapports entre sens et transparence. Ce concept entre par la porte ouverte par Trigano qui critique, on vient de le voir, la transparence comme processus univoque de découverte d'une vérité préexistante, et il permet d'explorer davantage ce qui est à l'œuvre dans l'auto-transparence.

Weick définit son concept en utilisant des notions voisines, et en circonscrivant peu à peu l'originalité du "sensemaking" par rapport à ces notions plus classiques. Ainsi, Weick identifie les ressemblances et les différences entre "sensemaking" et "interprétation". L'interprétation, selon lui, fait partie du sensemaking mais ne s'y limite pas. En effet, dans l'interprétation, l'information qui doit être interprétée est *donnée,* tandis que dans le sensemaking, les informations sont extraites par les acteurs, le processus même du choix des informations pertinentes en fait partie ("*what is left unspecified (in the interpretation notion) are how the cues got there in the first place and how these particular cues were singled out from an on going flow of experience*"). De même, dans l'interprétation le sens préexiste, et doit être découvert, alors que dans le sensemaking, le sens est crée. ("*Sensemaking is about authoring as well as interpretation, creation as well as discovery*"). Enfin, le SM serait plutôt de l'ordre du processus, et l'interprétation du résultat produit. Enfin, quoique ceci nous paraisse peut être sujet à discussion, Weick considère que le "sensemaking" est plus "engageant" pour l'acteur, alors que l'interprétation serait l'œuvre d'un sujet intrinsèquement plus passif[48]. ("*Interpretation connotes an activity that is more detached and passive than the activity of sensemaking*").

La notion centrale dans le processus de sensemaking est la notion d' *enaction :* je crée l'objet à voir et à inspecter quand je dis ou fais quelque chose ("*I create the object to be seen when I say or do something*"). L'énaction produit l'environnement : elle produit des catégories, des objets, elle délimite des frontières qui ne préexistaient pas. Donc, pour le reformuler dans nos termes, l'objet de l'auto-transparence ne préexiste pas, il se construit.

Par exemple, dans le domaine des risques, l'information ne préexiste pas en tant que telle : on choisit de regarder des incidents, on décide qu'un incident est une perte de séparation, mais cette catégorie de l'objet "incident" est énactée par l'organisation, qui décide de regarder ces objets-là, et non d'autres. Suivant la compréhension de la sécurité, on ne regarde pas les mêmes objets ou on regarde

[47] Karl Weick : *Sensemaking in organisations*. Sage Publications. 1995.

[48] Ce dernier point nous paraît discutable car, par exemple, l'interprétation littéraire ou artistique est très *engageante* pour le critique. Par exemple, lorsque Siri Hustvedt interprète le tableau de Vermeer : *la femme au collier de perles* comme une *annonciation*, elle propose à ses lecteurs une nouvelle vision qui n'a rien de passif. Siri Hustvedt. *Yonder.* Henri Holt. 1998.

les mêmes objets mais en leur donnant un sens différent. Cela dépend notamment du paradigme (au sens que lui donne Laroche[49]) de l'organisation.

2.5. Conclusion

Aborder la transparence sous l'angle philosophique permet de souligner le lien entre cette notion et la Modernité, et son projet d'un monde rendu transparent à lui même. Le point de vue de la science politique replace la transparence au sein des institutions et l'analyse principalement comme un principe régulateur, par exemple comme un contre-pouvoir des citoyens envers leur gouvernement. Les juristes rappellent que la "*notion molle*" de transparence peut se transformer assez vite en question "*dure*" ! : "*qui décide de ce qui est rendu transparent à qui* ?". Cette question opère en effet un arbitrage entre l'intérêt des uns et des autres, et détermine un équilibre entre les pouvoirs. Enfin, il existe des différences entre les démocraties occidentales, dans lesquelles il n'existe pas d'arbitre "naturel" ou du moins communément accepté quant au contrôle final de la transparence (pouvoir des autorités indépendantes en France, versus pouvoir du juge aux Etats Unis par exemple). L'étude de ces aspects macroscopiques permet d'anticiper que les mêmes questionnements devraient se retrouver à un niveau organisationnel, avec le cas des organisations à risques, avec des spécificités qu'on se propose de détailler dans le chapitre suivant.

Enfin, une approche plus sociologique a permis d'introduire des notions annexes (vie privée, secret, intimité, confiance) qui permettent d'aborder le point de vue des acteurs sur la transparence. Ces notions prennent elles aussi une nouvelle dimension dans les organisations à risques.

[49] Hervé Laroche utilise la définition de Gerry Johnson : l'ensemble des croyances et des hypothèses relativement communément répandues dans l'organisation, considérées comme allant de soi, et perceptibles dans les histoires-explications des managers, qui jouent un rôle central dans l'interprétation des stimuli environnementaux et dans la configuration des réponses stratégiques organisationnellement pertinentes. "*Risques, crises, et problématique de la décision dans les organisations*". Séminaire du programme Risques collectifs et Situations de crise. 15 Novembre 1995.

Chapitre 3.
Les organisations à hauts risques : enjeux spécifiques de la transparence

(...) Un hedge funds, un fonds spéculatif, qui s'appelait LTCM, capital management, donc avant les hedge funds on savait pas ce qu'ils prenaient comme positions, ils étaient jaloux de leur stratégie, tout ce que tu savais c'est que tu mettais de l'argent, ils prenaient des très grosses pos, très risquées mais d'un autre côté, tu avais des perspectives de gains qui n'avaient rien à voir avec une sicav action, tu t'attendais à faire, 30, 40, 50 ... ou alors à tout perdre. Le problème, c'est que tous ces fonds-là publiaient rien, on ne savait pas ce qu'il y avait dedans, et après la quasi faillite de LTCM, ça a incité à la transparence.

Un trader.

3.1. Introduction

Dans ce chapitre, on se propose de se centrer sur la question dans la transparence dans un domaine précis : les organisations à hauts risques. Concrètement, il s'agit de reposer les éléments théoriques présentés dans le chapitre précédent en fonction de leur pertinence pour ce type d'organisation.

Les questions théoriques reprises ici sont :

1. Quel sens prend la notion d'*auto-transparence* dans une organisation à risques ?
2. Si on prend "transparence" dans le premier sens (*la transparence d'une organisation*), quels liens nouveaux peut-t-on faire entre transparence et confiance ?
3. Si on prend "transparence" dans le deuxième sens (*la transparence de l'individu*) : quel enjeu nouveau prend la transparence du professionnel lorsque celui ci travaille dans une organisation à risques ?

3.2. L'*Auto-transparence* comme objectif

Dans le chapitre précédent, on a vu avec Vattimo qu'un projet d'*auto-transparence* était à l'œuvre dans la modernité. Ce projet est aussi lié à la rationalisation au sens Weberien. Comment ce projet prend-il sens et se développe-t-il dans une organisation à risques, qui peut sans doute être considérée comme un pur produit de nos sociétés industrielles ?

Une organisation à risques peut se conceptualiser comme Macro Système Technique. Alain Gras[50] propose de combiner les apports de Luhman (le système est un tout cohérent, doté de propriétés comme le feed back), et de Hughes (le système est aussi un *réseau de pouvoirs*, il est un lieu de conflit d'intérêts des acteurs sociaux) pour forger le concept de Macro Système Technique. Ce concept permet de comprendre l'existence et la croissance de nouveaux "sujets-objets" historiques.

Le Macro système Technique

Une des caractéristiques du MST est d'être "*éclaté*" : il est composé de multiples sous systèmes, qui peuvent être géographiquement éloignés, de très nombreuses personnes, aux compétences et rôles très différents), *etc.* mais, grâce à l'information, concept clef du MST, "*l'ensemble du MST est présent à lui même*". Dans le même temps, "*Le macro système est toujours branché sur un imaginaire qui le dépasse*". Il existe donc à la fois, une sorte d'auto-transparence (l'information circule dans le réseau, permettant un mécanisme d'auto régulation, donc, pour le dire en termes un peu trop organicistes, le système *se connaît lui même*) mais aussi une forme d'opacité car ce même système s'ancre dans un imaginaire, qui le transcende.

La question posée ici en filigrane, est : "*quel est le degré d'auto conscience d'un macro système Technique ?*" ou plus exactement, puisqu'un système est aussi composé d'humains : "*quelle est la nature de la connaissance que des humains peuvent obtenir d'un système complexe*" ? Si cette connaissance est distribuée chez les différents acteurs qui ont tous un point de vue idéologique (au sens de Mannheim) comment pourrait s'opérer une synthèse, sur un risque par exemple ?

Sur ce sujet, Alain Gras s'interroge en Anthropologue (communication personnell(nne)-5ll(ng0.8.3(: un t)-21.7(

transparence" totale, de rationalisation, qui est à l'œuvre dans les différentes approches d'ingénierie de la sécurité.

Le secret structurel

Sur le même sujet, Diane Vaughan s'interroge en sociologue. Elle montre, dans son analyse de la catastrophe Challenger, comment une organisation peut devenir aveugle à ses propres risques. Diane Vaughan ne pose pas la question de l'*essence* du projet d'*auto-transparence*, elle prend l'angle de l'analyse organisationnelle et anthropologique pour montrer comment une organisation particulière (la NASA) a construit une opacité sur son propre fonctionnement qui conduit à la catastrophe que l'on connaît (Challenger) en 1986.

Diane Vaughan élabore la notion de "secret structurel"[51] pour caractériser le fonctionnement de la NASA. Elle fait de cette notion une des clefs[52] pour comprendre pourquoi la décision de lancement de la navette fut prise, en dépit d'éléments, qui, a posteriori, apparaissent alarmants. Ce secret identifié est structurel, et non individuel : les personnes n'ont pas *volontairement* souhaité dissimuler des informations critiques, c'est toute l'organisation, qui, dans sa construction formelle et son fonctionnement, entraînait un affaiblissement des signaux, une dilution de la perception des risques.

Ce secret structurel a travaillé à ce que Vaughan appelle "*la normalisation de la déviance*" : "*progressif*[53] *et systématique dépassement des bornes de l'acceptable par le groupe*". Les trois sources de ce secret sont, selon elle :

- ➔ (1) les signaux du danger étaient affaiblis par le processus d'analyse même de ces signaux, de signaux forts, ils devenaient des signaux faibles; les tests, par exemple, ne permirent pas d'identifier une relation causale entre la température et l'érosion des joints, en raison de la variabilité des résultats.
- ➔ (2) la structure de l'organisation, pourtant prévue pour "faire circuler l'information" arrivait plutôt à l'inverse de l'effet recherché, une très grande quantité d'informations circulait, "un blizzard de papier"*…* Le langage employé a aussi son importance, "le langage sur le risque, dans la culture de la NASA, était par nature technique, impersonnel, et bureaucratique" explique Vaughan, le mot "catastrophe", par exemple, qui paraît fort, était souvent mentionné dans différents papiers produits puisque utilisé de façon routinière pour un certain type de panne.
- ➔ (3) les relations de la NASA avec les régulateurs, interne et externe, résultaient en un mélange d'autonomie et d'interdépendance, qui ont inhibé la capacité de ces derniers à construire une représentation du risque qui soit fondamentalement différente de celle de la NASA.

On peut dire que chez Diane Vaughan, le secret structurel se construit à la fois sur des caractéristiques formelles de l'organisation (ce qui est prévu en termes d'organisation, de partage des rôles, de responsabilités) et sur des pratiques qui se développent peu à peu, et dont elle reconstitue l'historique.

L'organisation générative : Une transparence possible ?

Ron Westrum[54], sociologue également, utilise des caractéristiques formelles et des pratiques pour décrire des "idéaux types", pour reprendre une formule commode, d'organisations.

---

[51] Diane Vaughan *The Challenger Launch Decision.* Chicago Press. 1996.

[52] Une des clefs, mais pas la seule : les autres éléments ne sont pas centraux par rapport au questionnement sur la Transparence.

[53] Le caractère *progressif* explique que la sonnette d'alarme ne soit pas tirée, parce qu'il n'y a pas de conscience véritable, de la part du collectif, que l'on a modifié son point de vue sur ce qui était considéré comme acceptable (l'on s'est mis à admettre ce qu'on n'admettait pas auparavant par exemple). D'autre part, le caractère *systématique* de la déviance renforce l'oubli de la norme qui avait été retenue pour différencier l'acceptable de l'inacceptable.

[54] Ron Westrum. Westrum, Ron. (1991). *Technologies & society: The shaping of people and things*. Belmont, CA: Wadsworth Publishing Compan.

Il distingue trois types d'organisations dans lesquelles on peut lire des degrés de transparence différents quant à la gestion des informations critiques[55]. Les organisations pathologiques sont particulièrement opaques, les informations sont simplement cachées. Les organisations bureaucratiques gèrent les informations, mais pas de façon très utile et opératoire, et enfin les organisations génératives cherchent activement les informations elles sont en quelque sorte les organisations idéales, qui réalisent une forme de cette *auto-transparence*, de cette connaissance de l'organisation par elle même. L'organisation générative, en effet, est une organisation apprenante, qui décode les *signaux* au sens de Diane Vaughan et agit en conséquence. Il faut bien noter que l'organisation générative n'est pas transparente au sens restreint du terme, et surtout elle n'est *seulement* transparente : l'information circule, mais surtout elle "fait sens".

Cependant, cet idéal comporte un enjeu de taille : c'est la question soulevée par Alain Gras lorsqu'il remarque que "*l'organisation générative et sa transparence se heurteraient toujours à la dimension politique de l'organisation*".[56] Ce qui a été abordé dans les visions politiques et juridiques du chapitre précédent : la transparence trace aussi un équilibre des pouvoirs.

En conclusion

Le projet de la transparence, au sein même de l'organisation à risques, peut être questionné, de façon fondamentale, essentialiste, avec la notion de macro système technique, en lien avec les réflexions sur la modernité. A un niveau plus concret, il peut aussi être abordé en des termes socio organisationnels : c'est ce que propose Diane Vaughan, avec le cas de Challenger, dans lequel elle reconstitue la construction d'un secret *structurel* au sein d'une organisation. C'est aussi en termes socio-organisationnels que Ron Westrum aborde une typologie d'organisations plus ou moins "transparentes", dont on peut montrer une limite cette fois-ci politique.

3.3. Transparence de l'organisation : la construction de la confiance

Cette partie aborde la transparence d'une institution vis-à-vis d'un "extérieur" : ici, une organisation et un public extérieur. Souvent une organisation à risques concerne tous les citoyens, pas seulement les usagers du système en question. Le chapitre précédent a permis de montrer que les liens entre transparence et confiance se reposaient de façon nouvelle dans une société industrielle produisant des risques complexes. On s'accorde à ce qu'il y ait un degré requis de transparence pour instaurer la confiance, mais, contrairement aux sociétés traditionnelles dans lesquelles Simmel a montré qu'un consensus sur le "quantum de savoir et de non savoir" s'établissait peu à peu, les sociétés modernes sont bien démunies pour s'accorder sur ce "quantum d'information". La complexité des domaines, la nature même des risques sur lesquels les scientifiques ne s'accordent pas, rendent la tâche infiniment plus ardue.

La transparence serait peut être alors réclamée à corps et à cris dans certaines affaires récentes par les citoyens, comme symptôme d'une perte de confiance, et pas uniquement comme un moyen rationnel d'assurer un contrôle des risques. Le fameux principe de précaution peut être conçu comme une réponse possible à cette perte de confiance : au delà de son caractère rationnel (éliminer un risque même s'il n'est pas avéré), il a aussi peut être un sens symbolique : instaurer ou restaurer une forme de confiance, en remplaçant une transparence impossible par une décision forte et visible.

Dans les organisations à hauts risques, les autorités réglementaires jouent notamment ce rôle d'intermédiaire entre une organisation fournissant un service et les citoyens. A noter que cette autorité séparée existe de longue date pour certaines industries (exemple, le Nucléaire), et vient seulement de se mettre en place dans d'autres : c'est le cas pour le contrôle de Trafic aérien, avec la séparation désormais souhaitée entre le fournisseur de services de contrôle et une autorité réglementaire indépendante.

---

[55] Comme pour D. Vaughan, cette lecture de R. Westrum est restreinte à l'angle de la transparence.

[56] Alain Gras *Anthropologie et sécurité,* Colloque sur les Risques. Gif-sur-Yvette. 1999. C'est d'ailleurs à partir de cette réflexion que s'est amorcé le travail décrit dans ce document.

Cependant, peu de travaux théoriques existent sur la construction de cette confiance, et la médiation éventuelle apportée dans cette construction par une autorité de régulation séparée. Todd La Porte, avec sa notion de "constance institutionnelle", aborde la construction de la confiance entre une organisation à haut risques et le public. Elle se définit comme "adhésion fidèle, inflexible aux actions effectives et aux engagements à travers plusieurs générations"[57]: "*Il ne s'agit pas de ne rien changer mais au contraire de permettre des évolutions tout en restant fidèle au pacte originel, qui garantissait qu'un soin toujours renouvelé sera toujours donné aux activités de manière à empêcher toute dérive ou toute action qui compromettrait d'une façon ou d'une autre les niveaux de fiabilité et de sécurité*"[58]. La Porte pose notamment la question d'une forme de transparence de l'organisation vis-à-vis des autorités de sûreté.

3.4. La transparence "de l'individu" : qu'est-ce qui est acceptable ?

Cette dernière partie repose le problème de ce que nous avons appelé "la transparence de l'individu", et aborde les questions liées à la vie privée ou plutôt à l'intimité, à ce que les anglo-saxons nomment "privacy", en se restreignant au monde du travail. Dans certaines organisations, il s'agit avant tout de surveiller le système et ses incidents dans une perspective d'apprentissage organisationnel. Mais les incidents peuvent être liés à des actions faites par des personnes, la distinction est par conséquent ténue… Plus qu'ailleurs, sans doute, le professionnel accepte une forme de *surveillance* et de contrôle de ses activités, mais jusqu'où ? Et qui a la légitimité de fixer la limite ?

Les domaines ont été volontairement choisis hors du contrôle aérien qui fait partie d'un développement spécifique dans les chapitres suivants. Quel est le *sens* de cette surveillance pour un professionnel ? Quel est le degré d'acceptabilité ? de quoi dépend-il ? ces questions seront rapidement abordées à travers deux cas concrets. Le premier concerne l'aéronautique avec les pilotes de ligne, le second le monde des opérations boursières Enfin, la question plus politique de la limite démocratique du contrôle est posée à partir des réflexions de Charles Perrow.

Les pilotes : du techniquement faisable à l'acceptable

Plusieurs systèmes permettent d'enregistrer des données de vol : les échanges entre le contrôle aérien et les pilotes, (Cockpit Voice Recorders), mais aussi l'analyse des vols. Connu dans le monde Anglo Saxon sous le terme de FOQA, l'enregistrement des paramètres de vol permet une comparaison continue entre le profil de vol, et les paramètres des moteurs et de divers systèmes, et un ensemble de paramètres préétablis qui constituent une enveloppe. Certains évènements-sécurité (ou incidents dans la terminologie que nous avons utilisé jusqu'alors) sont détectés sur un seul paramètre, tandis que d'autres utilisent la combinaison de plusieurs paramètres et des algorithmes complexes[59]. Certaines compagnies Aériennes comme British Airways et Air France utilisent ces systèmes depuis plusieurs décennies. Des incidents tels qu'un décollage abandonné, une vitesse d'approche trop rapide, ou la déviation de la trajectoire de guidage de l'ILS sont ainsi automatiquement détectés. Tous les vols sont systématiquement dépouillés et pour chaque incident identifié, un questionnaire est envoyé à l'équipage[60].

La réglementation JAR rend obligatoire l'analyse des vols pour toute compagnie ayant des avions de plus de 10T[61]. Au moment de sa mise en place, ce système a soulevé des questions quant à la surveillance ainsi exercée sur les équipages. A Air France par exemple, des procédures ont été discutées entre la compagnie et les associations professionnelles de pilotes afin d'assurer une confidentialité (ici un système de double enveloppe, qui assure la confidentialité de l'équipage, mais non l'anonymat, qui ne permettrait pas, bien sûr, de collecter le point de vue de l'équipage sur l'incident et son contexte). British Airways a aussi établi un accord avec l'association des pilotes, selon

[57] *Faithful, unswerving adherence to commitments and effective actions over many work generations*.
[58] La Porte. Colloque CNRS sur les Risques. Gif sur Yvette. Mai 2001
[59] Explications d'après un article de Mike Holton : Holton (Captain Mike Holton). FOQA : Aviation's most important safety tool. British Airways. 52 FSF Annual International Air Safety Seminar, 29th IFA international conference and IATA. November 1999.
[60] Interview de Monsieur Martegoutte, responsable du département d'analyse des vols à Air France.
[61] JAR OPS paragraph 1.037 makes mandatory Flight data Analysis for any airline having Aircraft > 10 tons. Thank you to Claire Pelegrin for information provided.

lequel "la seule occurrence d'un événement d'un analyseur de vols ne saurait constituer la base d'une action disciplinaire"[62].

L'utilisation d'enregistreurs vidéo dans les cockpits est à l'étude, ce qui repose de façon plus aiguë la question de la limite acceptable pour les pilotes de la surveillance de leurs actions. Ces enregistreurs vidéo seraient capables de collecter des informations non enregistrées par les enregistreurs de données de vol et les informations qui ne sont pas liées aux instructions du contrôle aérien. L'ALPA (association des pilotes de ligne) aux Etats Unis défend un enregistrement vidéo limité aux actions faîtes sur les instruments de bord, tandis que le NTSB (National Transport Safety Booard) préfèrerait enregistrer l'image de toute la cabine, y compris les comportements des pilotes. Lindsay Fenwick, un des membres de l'ALPA argumente : "*nous devons trouver un équilibre entre ce qui est technologiquement faisable et ce que les investigateurs voudraient avec les questions fondamentales de la vie privée*"[63].

Le Trading : la transparence comme régulation du risque

Les personnes chargées des opérations de trading ont pour métier de faire fructifier l'argent d'un organisme, d'une banque, par exemple, en spéculant sur les hausses et baisses du marche boursier. Le travail de ces personnes se déroule dans une bonne dose de transparence : les conversations téléphoniques sont enregistrées, les logiciels qui permettent d'effectuer les opérations d'achat et de vente sont archivés chaque soir, afin de permettre le débriefing du lendemain matin. Chaque trader est contraint par une certaine limite de risque qui lui est assignée par le chef de l'unité dans laquelle il opère (le desk manager). Cette limite est individuelle, et laissée à la discrétion du Desk manager, quoique des dépassements de cette limite soient toujours possibles, et discutés au cas par cas entre le trader et son responsable.

Dans ce métier, plusieurs aspects nous paraissent très intéressants au regard de notre problématique.

L'acceptabilité (le caractère juste de la surveillance) est extrêmement liée au caractère risqué du métier. Un Trader nous explique :

"*Le trading c'est une culture de risque, tu es payé pour prendre des risques, d'un autre côté, t'acceptes aussi qu'il y ait des gens qui aient envie de savoir ce que fais, quoi… cela va ensemble*"

La surveillance est des lors considérée comme une sorte de garde fou, pour l'organisation, mais aussi pour le trader lui même. On le comprend à demi mots, le risque est un plaisir, une valeur centrale, mais sans ce garde fou, il serait facile de céder à une ivresse certaine. On y met des limites, et ces limites sont personnelles.

Il existe aussi une régulation collective (puisque le chef de Desk opère lui même en prenant en compte les risques pris par son équipe).

"*(…) si tu prends une grosse pos, sur un truc généralement t'y crois parce que t'en parles avec ton boss qui est juste a cote de toi et il te dit oui ou non… après lui il répond en fonction de la position globale de l'ensemble des traders et il dit "non maintenant on est tous déjà super exposés sur ce truc, je préfère pas", lui il peut te laisser, s'il te trouve surexposé, il peut prendre une position sur le marché de façon à réduire le risque sur l'ensemble du desk, par exemple, si on est tous long du marché, on a tous pris des actions comme des malades, et lui il pense qu'on est vraiment trop longs, que cela va pas vraiment monter, lui pour gérer le risque de l'ensemble des positions des traders, il peut vendre du CAC ou n'importe quoi en face de façon à réduire le risque global du desk*"

---

[62] "Evidence from a Flight Data Recorder alone will not constitute a basis for any disciplinary hearing or action.

[63] *We need to balance what is technologically feasible and what investigators would like with the fundamental privacy issues.* Fenwick Lindsay. Access to data : Privacy, Proprietary and Unions Issues.. International Symposium on Transportation Recorders. Arlington. 1999.

Dans certaines banques, les traders doivent effectuer un rapport chaque matin de leurs opérations, rapport qui consiste notamment a justifier de leurs actions.

"*Nous on a en plus à la banque X qu'on ne fait pas chez Y, on envoie un email au responsable du desk qui explique : quelles sont nos positions, qu'est ce qui reste, quel résultat, par exemple, aujourd'hui j'ai perdu ou gagné, 200 ou 300 000 dollars, pourquoi, comment, parce que, au delà de 100 000 dollars de gains ou de pertes on doit mettre une explication sur pourquoi, comment*"…

Ce contrôle semble accepté notamment parce que le professionnel, en explicitant sa stratégie, éclaire aussi pour lui même ce qui était parfois de l'ordre de l'intuition. Un peu comme s'il était aussi plus transparent à lui même :

"*Oui, parce que ça te pousse aussi à plus réfléchir sur quelles pos tu prends, pourquoi… des fois tu peux te dire, tiens TOTAL, le pétrole, çà barde au moyen orient, mais je ne pense pas que ça va durer, donc j'en vends 2 millions, et puis cela monte et tu perds je sais pas 200 000 dollars, faut quand même t'expliquer : c'est quoi ta vision, quand tu prends une pos et qu'on te dit : pourquoi cette pos ?, tu racontes une histoire : tu dis voilà mon scénario et tout ça, si jamais il revient 2 ou 3 jours après, t'as toujours la pos, mais ça va contre toi depuis 3 jours, je pense que t'as tort (rires)…*"

Il existe tout de même une marge d'opacité, des opérations peuvent être cachées car le monde des opérations boursières est de plus en plus complexe. Cependant, il existe un accord (qui nous apparaît comme une sorte de code d'honneur de la profession) sur ce qu'on peut cacher a la rigueur, (les gains) et ce qu'il est interdit de cacher (les pertes).

"*Il y a des moyens, parce que c'est tellement compliqué à partir des produits qu'on traite, tu peux toujours, tellement les modèles sont compliqués, paramétrer de façon à ce que ça ne dépasse pas les limites, tu peux toujours le faire, plus c'est compliqué, plus c'est facile de cacher des pertes ou de mettre de côté des gains, pour l'avenir, cela, c'est toujours possible,*

Tu mets toujours un petit peu d'argent de côté, pour les vaches maigres…

Tu mets de côte pour le mois d'après parce que tu sais pas comment ça va se passer, mais cacher des pertes, non , c'est vraiment pas la culture, (…) si jamais tu caches des pertes, tu es viré sur le champ, t'as 10 minutes pour prendre tes affaires personnelles et partir… "

Cette transparence accrue est relativement récente, elle s'est mise en place peu à peu, et bien sûr, elle n'est pas sans influencer le comportement des traders…

"*C'est progressivement, en fonction du développement du marché, des grandes affaires qu'il y a eu en termes de pertes, les contrôles ont été accrus à la fois en termes de systèmes et par le département des risques, les opérations, tout ce qui est autour du trader, tout cela s'est étoffé à la fois en termes technique, humain, contrôle des positions, et cette pression çà te force toi à être plus à faire plus attention, c'est un peu vertueux en termes de contrôle des risques.*"

Quant aux fonds communs de placement, ils ont longtemps pu être opaques… tant qu'ils ont été capables de gagner de l'argent. En 1999, la faillite retentissante du LTCM a alerté le monde financier, et déclenché la mise en place d'une plus grande transparence sur les opérations effectuées : il s'agit d'opérer une forme de surveillance continue des performances d'investissement, afin de pouvoir réagir rapidement. Il restera toujours des zones d'opacité : les paradis fiscaux…

3.5. Les limites du contrôle : le souci démocratique

Ce dernier paragraphe aborde les questions de la surveillance des professionnels dans une perspective plus politique. Dans "Les limites de la sécurité", Scott Sagan a comparé deux courants qui s'opposent quant à l'analyse des organisations à hauts risques. Pour le résumer de façon très rapide, d'un côté, le courant des "organisations hautement fiables" abrégées en HRO (High Reliability Organisations")

considère que des éléments de nature essentiellement organisationnelle (organisation du travail, entraînement, retour d'expérience,…) permettent de dépasser les risques intrinsèques dus aux activités à haut risques comme le nucléaire ou l'aéronautique. De l'autre côté, les tenants de l' "accident Normal", dont la théorie a été élaborée par Charles Perrow, considèrent que ces organisations sont structurellement amenées[64] à provoquer tôt ou tard un accident : l'accident "Normal". Sagan oppose la description des HRO qu'il décrit comme des systèmes clos, largement sinon totalement soustraits aux influences extérieures, à la vision de ces mêmes organisations par Perrow, systèmes ouverts, au cœur d'un environnement essentiellement imprévisible et complexe, qui sont autant de périls potentiels pour la fiabilité.

On peut lire en filigrane, que les chercheurs des HRO ne se centrent pas sur la question du "contrôle" des individus, alors que cette question est centrale pour Charles Perrow. Pour ce dernier, en effet, les HRO n'obtiennent des résultats satisfaisants en termes de fiabilité qu'au prix d' "*un contrôle des individus incompatible avec la démocratie*".

Dans un tableau où il compare les deux courants, Sagan exprime la controverse sous cette forme. Pour les HRO : une culture de sécurité[65] (…) en encourageant des réponses uniformes et appropriées de la part des opérateurs". Pour la théorie de l'accident normal : "un modèle militaire de discipline intense, de socialisation, et d'isolement est incompatible avec des valeurs démocratiques[66]".

Radicalisant sa compréhension de l'organisation HRO "fermée", Sagan se réfère également au concept *d'institution totale* élaboré par Goffman : "*un grand nombre d'individus coupés d'une société plus grande, qui mène à un mode de vie formellement administré*"[67]. Il insiste sur le caractère "normalisant" des organisations décrites par les théoriciens des HRO : c'est un contrôle de tous les instants, qui modèle les conduites des individus, de façon essentiellement insidieuse, et d'autant plus efficace. On peut noter toutefois que Sagan donne pour seul exemple lorsqu'il mentionne cette parenté avec l'institution totale, le domaine des porte-avions militaires (isolement, socialisation intense, culture militaire, *etc.*). Les caractéristiques de l'institution totale ne sont pas pertinentes lorsqu'il s'agit d'autres organisations pourtant également estampillées "HRO" par nos théoriciens : les centrales nucléaires, le contrôle de trafic aérien, dont les membres ne sont ni isolés, ni militarisés…

Cependant, Perrow et Sagan soulèvent une vraie question, si on l'exprime en des termes moins radicaux : les organisations à risques impliquent peu ou prou une forme de contrôle des professionnels, mais quelle est la limite de ce contrôle[68] ? S'il subsiste toujours pour un professionnel une "marge d'opacité" comme l'appelle Friedberg, et ceci y compris dans l'Institution Totale de Goffmann, on manque peut être de réflexions sur le *sens* que le professionnel donne à ce dosage entre transparence et opacité. On manque aussi de réflexions sur ce qui pourrait fonder les bases d'un consensus entre les professionnels directement impliqués dans la prise de risque, leur hiérarchie, les autorités réglementaires et le public.

Pour amorcer très succinctement ce débat, il semble clair que la transparence (du moins, un certain degré de transparence) de l'individu au travail n'est acceptée que si elle réalise un équilibre entre l'intérêt apporté par la modalité de surveillance et la perte d'intimité qui en résulte. C'est bien ce qu'affirme Lindsay Fenwick à propos des vidéo dans les cockpits. La jurisprudence en matière de droit

---

[64] Parce que, dit Perrow, ces organisations sont à la fois "étroitement couplées" et très complexes, et qu'aucune "solution organisationnelle" ne permet de pallier ces défauts. Cf. *The limits of Safety*. Scott Sagan.

[65] *A culture of reliability will enhance safety by encouraging uniform and appropriate responses by field operators*. The limits of Safety. Scott Sagan. *The limits of Safety.* Princeton University Press. 1993.

[66] A military model of intense discipline, socialization, and isolation is incompatible with democratic values. Op. Cit.

[67] A large number of like-situated individuals, cut-off from wider society, for an appreciable period of time, together lead an enclosed, formally administrated round of life". Asyliums : Essays on the social situation of mental patients, and other inmates. 1961

[68] Il existe sans doute aussi une variabilité très large de l'acception d'un contrôle. Par exemple, aux Etats Unis, "*Chez Dupont de Nemours, quelqu'un qui a été impliqué dans un événement accidentel dans son milieu personnel aura à s'en expliquer à sa hiérarchie au motif – que je partage mais j'y apporte des nuances - que la sécurité est un état d'esprit permanent*". Yvan Verot. Maîtrise du risque dans l'industrie chimique et pétrochimique : retour d'expérience. Séminaire CNRS. Mars 1998.

à l'intimité des salariés ne dit pas autre chose lorsqu'elle recommande la "proportionnalité[69]" de la surveillance aux objectifs de cette surveillance pour le bon fonctionnement du travail; elle ne peut s'exercer, en outre, à l'insu des salariés[70].

En outre, un professionnel peut accorder un sens à cette transparence, qui est tout autre chose qu'une simple acceptation résignée. Un trader que nous avons interrogé évoque la transparence comme un juste prix à payer en échange des risques qui sont pris, et celle-ci constitue semble–t-il même une forme de garde fou. La transparence (le contrôle) est ici acceptable par le professionnel à l'aune des enjeux qui sont soulevés, enjeux dont il est parfaitement conscient. D'ailleurs, dans son discours, notre trader replace "sa" transparence dans le cadre d'une transparence plus globale qui se développe pour toute l'organisation, dans un processus qu'il n'est pas le seul à "subir", et qu'il conçoit dans une perspective de progrès général sur la transparence financière. En conclusion, la transparence qu'un professionnel accepte sur son travail dépend aussi du sens qui est donné à cette transparence dans le collectif auquel il appartient.

En miroir, l'opacité du professionnel a aussi a un sens. Erhard Friedberg défend la nécessité de laisser au professionnel une marge d'opacité, mais il ne donne pas de sens à cette opacité[71]. Ses raisons sont plutôt d'ordre pragmatique : il existerait une sorte de résistance à la transparence totale qu'il est inutile de vouloir à tout prix instaurer. Il peut y avoir dans certaines situations un lien avec le pouvoir : on se souvient que le pouvoir dépend de la "zone d'incertitude" laissée à une personne. Mais dans le cas des situations professionnelles qui nous intéressent ici, qu'il s'agisse du trader, du pilote, ou par exemple, du contrôleur aérien, cette zone d'opacité ne consiste plus vraiment en "du pouvoir". Il s'agit d'une forme de maîtrise, d'autonomie dans son travail, certes, mais pas d'un pouvoir dans une relation avec autrui. Ceci étant dit, cette zone d'opacité n'est pas sans soulever aussi des questions quant à son impact sur le fonctionnement d'une organisation à risques, et, in fine, sur la sécurité du système. Ironie du sort, des professionnels peuvent être condamnés à cette opacité par les lacunes de l'organisation. Un exemple récent nous est fourni par Mathilde Bourrier[72] qui analyse la transgression des règles par les professionnels de la maintenance dans les centrales nucléaires. Si certaines de ces transgressions s'enracinent dans l'*incomplétude structurelle* des procédures, obligeant les personnes à improviser là où la règle n'existe pas ou ne convient pas, d'autres transgressions sont plutôt liées à un fonctionnement de l'organisation qui ne sait pas *penser* l'évolution des procédures, leur mise à jour, et condamne de ce fait les opérateurs à une "autonomie opaque". Or, cette opacité entraîne des différences de plus en plus importantes entre ce qui est censé être fait et ce qui est réellement pratiqué, et ce sans doute au détriment de la sécurité.

3.6. Conclusion

Dans une organisation à risques, la question de la transparence se pose avec une acuité nouvelle. On a effleuré les limites fondamentales, structurelles, politiques de l'auto-transparence, c'est à dire de la connaissance que l'organisation a de son propre fonctionnement, notamment en termes d'identification des risques. Avec l'exemple du trading, on a identifié le rôle des grandes crises dans l'évolution de la transparence, ce n'est pas un processus continu. Deuxièmement, les liens entre transparence et confiance se posent de façon nouvelle. Enfin, chaque professionnel donne sens à la "*transparence*" qu'il accepte sur ses activités en fonction du sens global qui est donné à cette valeur dans l'organisation, et de la toujours nécessaire marge d'opacité qu'il pourra gérer.

---

[69] L'article L. 122-35 du code du travail explique que (le règlement intérieur d'une entreprise) "*ne peut apporter aux droits des personnes et aux libertés individuelles et collectives des restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché*".

[70] Jugement du tribunal de grande instance de Paris du 7 novembre 1975. *Les contrôles et les surveillances ne doivent être considérées comme entièrement justifiés que s'ils sont connus du personnel et non pas s'ils sont mis en œuvre à son insu*.

[71] En effet, la notion d'acteur stratégique implique, entre autre, la notion d'un comportement utilitariste de l'acteur, mais sans "analyse a priori des valeurs qui prévalent ou devraient prévaloir : le sens du comportement utilitariste est progressivement enrichi par l'analyse". Donc le sens dépend de chaque cas particulier.

[72] Mathilde Bourrier. Le Nucléaire à l'épreuve de l'organisation. PUF, 1999.

Chapitre 4.
Des objets techniques, outils de la transparence

De sa naissance à sa mort, un membre du Parti vit sous l'œil de la Police de la pensée. Même quand il est seul, il ne peut jamais être certain d'être réellement seul. Où qu'il se trouve, endormi ou éveillé, au travail ou au repos, il peut être inspecté sans avertissement et sans savoir qu'on l'inspecte. Rien de ce qu'il fait n'est indifférent.

1984. Georges Orwell.

4.1. Introduction

Certains objets techniques peuvent devenir des outils de la transparence, ou en d'autres termes, leur finalité, c'est de montrer, de permettre d'accéder à des informations qu'une "simple" relation d'humain à humain, non médiatisée, ne permettrait pas de révéler. Dans ce chapitre, on tente d'analyser quelques exemples de ces objets techniques et comment ils sont liés à des modalités plus ou moins intrusives de la transparence.

4.2. Quelques exemples[73]

Internet

Les particuliers connectés à Internet sont exposés de ce fait à différentes formes d'intrusions.
L'intrusion désormais la plus célèbre est l'analyse de son comportement lorsqu'il navigue sur Internet. De nombreux sites gardent non seulement trace de ses différents passages (notamment grâce aux désormais célèbres cookies[74]) mais analysent son comportement (soit individuellement : comment ce fait-il qu'il soit allé trois fois voir ce produit dans le catalogue mais ne l'ait pas acheté), soit collectivement, mais aussi échangent ou croisent entre eux les informations commerciales recueillies explicitement (par des formulaires) ou implicitement (par le comportement). Ces pratiques ne sont peut-être pas si différentes de celles des fichiers que se sont toujours revendus certaines sociétés entre elles. Si le potentiel de cette technologie semble quasi-insondable, les coûts des systèmes sophistiqués sont cependant très élevés et il semble que finalement peu d'entreprises sont prêtes à investir les montants considérables que demandent souvent de telles applications. A noter également que la régie publicitaire en ligne Doubleclick, sans doute une des entreprises commerciales qui possède le plus d'information sur les internautes du monde entier, a annoncé cette année qu'elle renonçait devant la pression public à recouper ces informations pour constituer un portrait robot de quasiment chaque internaute de la planète.

Une forme d'intrusion subie en permanence par le particulier, beaucoup moins connue car plus discrète, est celle à laquelle il est exposé par les applications qu'il a achetées ou téléchargées, en lesquelles il a choisi d'avoir confiance, et qui se comportent comme des Chevaux de Troie, envoyant discrètement à travers Internet à l'éditeur diverses informations sur le poste sur lequel elles sont installées : adresse Internet, système d'exploitation, configuration, autres applications installées, ressources, *etc.* Cette pratique très courante a lieu le plus souvent à l'insu de l'utilisateur, qui ignore quelle utilisation est faite des informations recueillies. Il est à noter qu'en dehors de l'intérêt commercial évident des informations remontées, cette pratique permet également à l'éditeur de savoir qui utilise des copies de son produit, donc éventuellement de détecter des copies pirates.

Les entreprises subissent les mêmes intrusions que les particuliers, sans compter qu'elles sont particulièrement sensibles aux risques d'effraction par des pirates, ou aux virus, qui les exposent au risque de paralysie de leurs systèmes d'informations.

Elles sont également de plus en plus largement exposées à travers leurs sites Web. Leur concurrents ont appris à scruter l'ensemble du Web pour en tirer le meilleur parti commercial : recherche des collaborateurs-clé, benchmarking, études de marché, *etc.* Il est possible de tirer énormément d'information sur une entreprise en scrutant son site Web, mais aussi en recoupant avec ce qu'en disent tous les sites d'analyse financiers, éventuellement les sites de syndicats, la Presse, les pages personnelles d'anciens collaborateurs, *etc.*

---

73 Pour cette partie, un grand merci à Laurent Chaput, directeur technique Schlumberger-Sema Ile de France.
74 les personnes un tant soit peu versées dans l'informatique savent bien qu'il suffit d'installer un "firewall" pour empêcher ce mécanisme : il y a presque toujours une symétrie, une parade qui se développe dans un jeu d' intrusion/protection.

La Télévision interactive

Une autre exemple est relatif un changement de technologie pour un objet technique plus ancien, la télévision, changement de technique qui induit de nouvelles possibilités. Ainsi, la télévision par câble permet de savoir que Monsieur x est entrain de regarder tel programme télévisé, ce que la TV hertzienne ne le permettait pas. De plus, la télévision par câble permettant l'accès à des centaines de chaînes, on ne saurait laisser au pauvre téléspectateur le soin de zapper ou de consulter des centaines de pages de programme, il faut l'aider à choisir.

Un premier pas consiste à demander à ce téléspectateur ce qu'il aime en général, afin de lui proposer chaque jour une sélection personnalisée de programmes et de films. Mais l'objet technique qui fait le lien entre vous et votre télévision doit permettre d'aller plus loin, et de dresser votre profil *implicite*. Ainsi, des recherches actuelles sur la TV interactive cherchent ainsi à dresser le profil d'un téléphile en prenant en compte, non seulement ce que celui ci déclare aimer dans un questionnaire idoine, mais aussi ce qu'il regarde effectivement. Le logiciel qui enregistre et analyse ce que la personne regarde vraiment est ainsi capable de proposer des programmes vraiment *adaptés aux goûts véritables* de l'utilisateur, étant entendus que ceux-ci ne sauraient se réduire aux préférences qu'il exprime explicitement… Par exemple, vous avez déclaré dans votre questionnaire que vous aimiez les émissions de Jazz, les documentaires animaliers et les films russes en VO, mais hier vous avez passé plus d'une heure à regarder un jeu stupide, alors à toutes fins utiles, dans ma sélection de ce soir, moi, objet technique perspicace, je vous propose aussi quelques jeux… (A quand le dévoilement de ce que vous souhaiteriez regarder inconsciemment sans avoir encore osé passer à l'acte… !).

Un pas supplémentaire est franchi avec le "*collaborative profiling tool*" , objet de recherches actuelles, qui propose une sélection encore plus fine à partir de l'analyse de votre profil personnel, comparé au profil (ensemble de données sur les goûts, caractéristiques sociales, *etc.*) de milliers de spectateurs enregistrés dans une base de données, cette comparaison permettant de déterminer encore mieux ce que vous êtes susceptibles d'aimer vraiment. Par exemple, vous n'aimez pas les westerns, or, les personnes qui ont le même profil que le votre, et qui ont déclaré ne pas aimer les westerns non plus, ont aimé "Dead Man" de Jarmush. Par conséquent, je vous propose ce film.

A travers ces différents outils liés à la télévision, on constate comment, peu à peu, l'objet technique télévision que l'on se bornait à allumer après avoir jeté un œil dans un programme, se dote peu à peu de prothèses intelligentes, qui rendent vos goûts et vos désirs anticipables, calculables, en un mot, transparents.

Blue eyes

La technologie Blue eyes de IBM a été crée avec la volonté d'enrichir les capacités perceptives des ordinateurs, afin d'améliorer la communication entre l'utilisateur et son ordinateur. Ce logiciel permet la capture vidéo d'expressions du visage et leur analyse, ainsi que l'enregistrement d'éléments sonores. En capturant l'état physique et émotionnel de la personne, l'ordinateur est capable de répondre plus efficacement aux attentes de l'utilisateur (par exemple dans des outils didactiques qui dès lors, seraient capables de comprendre qu' on ne comprend plus !) Ils instaurent un dialogue plus naturel, en mimant une partie de la communication entre humains.

Ce qui est en jeu une fois de plus ici, c'est bien un humain devenant plus transparent à la machine, en tout cas d'une forme de transparence, une lecture de signes qui était jusqu'alors réservée au dialogue entre vivants (car beaucoup d'animaux aussi sont capables de lire chez leurs congénères des états émotionnels).

Une fois de plus, c'est la collecte intensive et le recoupement de données qui vont permettre une utilisation mercantile de ces nouvelles capacités : cette technologie permet d'enregistrer de façon précise dans un supermarché, les personnes agacées par une promotion, dégoûtées par le parfum qui leur est présenté, *etc.* Il s'agit, finalement de doter les méthodes classiques du marketing de

nouveaux outils, mais on peut se demander si cette fois-ci, un tel outil ne change pas la nature même du procédé commercial.

Le directeur associe de l' ACLU (American Civil Liberty Union) explique à "la revue Technologique" : "*Bientôt vous serez capables de capturer non seulement combien de personnes se sont arrêtées, mais qui elles étaient. Une fois que l'identité sera établie, elle sera "cross-référencée" pour capturer les revenus et les préférences d'achat de cette personne*".

4.3. Le développement d'une critique

Toutes les critiques qui ne manquent pas de se développer en réponse à ces avancées techniques insistent sur le caractère intrusif de cette mise en transparence des individus. La référence au Panoptique de Foucault est assez classique, et plus encore l'évocation de "1984" d'Orwell, et de "Big Brother".

Il existe en France une commission bien connue, la CNIL[75]. Cette commission s'est penchée sur toutes les questions liées à la mise en œuvre de procédés de surveillance caméras, badges, accès au courrier électronique…). Le Rapport 1999 de la CNIL s'inquiète du développement de la "cybersurveillance", et de son influence sur le commerce électronique. En outre, il est de jurisprudence constante (de la Cour de cassation comme du Conseil d'Etat) que les procédés de surveillance sont illégaux dès lors qu'ils excèdent l'étendue des restrictions que l'employeur peut légalement apporter au droit des personnes et aux libertés individuelles, en particulier en l'absence soit d'une information préalable des salariés sur les contrôles opérés, soit de garanties que les contrôles sont effectués dans des conditions préservant la dignité et l'intimité (vie privée) des personnes[76].

Dans une veine plus humoristique mais néanmoins très sérieuse, il existe depuis peu des "Big Brother Awards" décernés par l'organisation non gouvernementale "Privacy international". Ces cérémonies décernent des récompenses bien peu appréciées des lauréats puisqu'il s'agit d'identifier les types de systèmes de surveillance mettant en péril les libertés individuelles. Il existe sept catégories pour ces prix (business-finance, politique, administration,…) qui sont décernés à des sociétés privés et à des organismes gouvernementaux. Ces trophées sont très liés au développement des nouvelles technologies : "aujourd'hui, il n'existe pas de loi fondamentale sur les libertés qui ne soit concernée par la révolution technologique", souligne, Thilo Weichert, le Responsable allemand de l'Association pour la protection des données, qui espère ainsi déclencher une explication sur la place publique[77].

4.4. Conclusion : une typologie d'outils ?

La transparence s'instrumente et ce n'est pas sans poser des questions sur le recul des libertés, de la vie privée. Mais il semble que la réflexion ait peu à gagner à poser de façon abstraite le rôle de ces outils dans une critique qui nivelle leurs différences pour mieux s'effarer de l'avènement d'un monde à la Orwell. Une approche plus "casuistique" permettrait peut être une critique plus pointue de ce qui est en jeu, à chaque fois, dans la mise en transparence : quel est l' "*intime*" dont il est question à chaque fois, (par exemple, l'intime de mon image n'est pas l'intime de mon profil de consommation),

[75] Commission nationale de l'informatique et des libertés, autorité administrative indépendante créée par la loi en 1978
[76] Denis de la Burgade, communication personnelle.
[77] Les trophées ont récompensé : la carte Payback, pour l'enregistrement abusif de données personnelles, le registre central des étrangers en Allemagne, les serveurs internet Apache, qui récoltent des données sur les internautes … voir le "Monde Interactif" du 1er Novembre 2000. Et aussi : http://www.privacyinternational.org. Cette organisation milite aussi pour le développement de FOIA. Où l'on voit que l'étudiante qui cherche des informations critiques sur les nouvelles technologies trouve quant même pratique de faire une recherche sur Internet …

quelle est la part d'exposition volontaire de l'individu, quelle est sa marge de manœuvre pour résister à l'intrusion, *etc.*

Il existe différentes modalités dans le "rendre transparent", par exemple :

- ➔ l'espionnage (l'objet révèle ce que je souhaitais cacher),
- ➔ la révélation (l'objet révèle et *objective* ce que nous savions déjà confusément),
- ➔ le dévoilement (l'objet révèle ce que des humains ne pouvaient pas appréhender sans son intervention).

Un même outil peut en outre pencher plus ou moins vers l'une ou l'autre de ces modalités de "mise en transparence" selon ce que les hommes en font. Un exemple concret sera fourni dans le chapitre suivant avec l'étude d'un outil de "surveillance de la sécurité aérienne".

Chapitre 5.
Le cas du contrôle de la Navigation aérienne

Les incursions pistes il n'y en avait pas, enfin, ce n'était pas un événement reporté. Quand je faisais ma collecte d'informations, les JAA faisaient une liste de "focus area", et "incursion de piste", c'était dans la liste américaine, pas dans la liste Européenne. J'ai appelé X. Je lui ai dit : "Pourquoi tu n'as pas mis les incursions de pistes ?" Il me répond : "non ce n'est pas un problème" ... alors je lui ai dit : "ah, bon, parce que tu n'as pas de données, tu n'as pas d'incidents ?" c'est devenu une plaisanterie ici.

Une responsable à la SRU.

5.1. Introduction au domaine

On se propose dans ce chapitre, d'appliquer les questions liées à la transparence à un domaine particulier, le contrôle de la navigation aérienne, terrain qui a généré puis accueilli cette recherche.
Le contrôle de la navigation aérienne est une "organisation à haut risque", et les questions abordées dans le chapitre 3 trouveront ici tout leur sens, même si on s'est restreint à une partie seulement des problèmes abordés quant aux enjeux spécifiques de la transparence.

Commençons par une petite description du domaine du contrôle aérien. Chaque jour, des avions décollent, survolent de longues distances, non pas tels des oiseaux, mais en suivant des routes aériennes car ils sont guidés par des systèmes de radio navigation au sol, ou des systèmes satellites, et atterrissent. Si des processus dits "stratégiques" permettent de limiter a priori l'encombrement du ciel, en imposant par exemple aux avions de ne pas décoller tous à la même heure, et de ne pas se retrouver tous à survoler le même endroit au même moment, un processus tactique reste nécessaire pour assurer "l'ordonnancement sûr, et efficace des avions".

Ce sont les contrôleurs de la Navigation Aérienne qui assurent ce travail, à l'aide d'un système technique complexe qui associe le traitement radar de chaque avion, et des informations dites "plan de vol" qui décrivent la trajectoire prévue de l'avion. Les règles de sécurité internationales imposent des séparations minimum entre les avions. Ces normes dépendent essentiellement de la qualité des infrastructures radar existant dans chaque pays : en Europe, ces normes sont généralement de 5 Miles Nautiques de séparation horizontale et 1000 (en dessous d'un certain niveau de vol) ou 2000 pieds (au-dessus) de séparation verticale pour les zones dites de contrôle en-route (c'est à dire, en gros, hors des phases d'atterrissage et de décollage). La séparation réglementaire des avions est assurée par un travail complexe d'analyse des situations et d'anticipation des trajectoires.

Dans la plupart des pays, un binôme de deux contrôleurs assure la surveillance d'une portion de l'espace aérien (un secteur de contrôle) pour ce qui est du contrôle en-route. Le premier donne des instructions aux pilotes grâce à une liaison radio; il donne ainsi le cas échéant des instructions aux pilotes telles que : prendre un cap, ralentir pour éviter un rattrapage, *etc.* lorsque la norme de séparation menace de ne plus être assurée. Le second prend en charge les coordinations : il s'assure des conditions d'entrée et de sortie du secteur de chacun des avions, et se coordonne avec les militaires qui sont aussi des usagers de l'espace aérien. Il existe également un contrôle d'approche, (zone intermédiaire entre le contrôle en route et la Tour) et un contrôle de Tour (décollage/atterrissage des avions, gestion des pistes, *etc.*).

Pour le contrôle en-route[78], la plupart des systèmes de contrôle aérien des pays Européens fournissent aux contrôleurs une alarme appelée "Filet de sauvegarde" ou "STCA" (Short Term Conflict Alert) : ce programme informatique calcule les futures séparations, et si la norme de séparation risque d'être enfreinte, fait clignoter les "étiquettes" des deux avions sur l'image radar du contrôleur. A noter qu'il ne s'agit pas d'un outil de *détection*, puisque la détection de conflits potentiels fait partie du travail du contrôleur, mais bien d'un système d'*alerte* destiné à signaler en dernier recours au contrôleur ce qui est souvent le résultat d'un raté (oubli d'un avion, mauvaise évaluation de la situation, pilote ne s'étant pas conformé aux instructions, *etc.*). De plus, c'est un outil *pour le contrôleur,* dont l'objectif est immédiat : corriger la situation, le risque de collision[79], et seul le binôme de contrôleurs (quelques collègues des secteurs adjacents, éventuellement) va être informé de l'incident.

[78] Le Filet de sauvegarde est à l'étude pour le contrôle d'approche, à Charles de Gaulle, mais non opérationnel.
[79] La France est pour le moment un des seuls pays en Europe, à notre connaissance, à avoir développé un système de recueil et d'analyse hors ligne de ces alertes Filet de Sauvegarde, et à essayer dans certains centres, de faire une analyse systématique de ces incidents, afin de comprendre la genèse de chaque incident. Ce qui sera détaillé dans le chapitre suivant.

5.2. Choisir un “objet” de la transparence

Dans une organisation complexe comme le contrôle de trafic aérien, la question de la transparence peut se poser à de multiples niveaux, pour de multiples objets (pourquoi pas la transparence financière, la transparence des décisions quant aux choix techniques, la transparence du calcul de la capacité des secteurs…). Par exemple, le projet TORCH, qui entend définir le concept opérationnel futur du contrôle aérien pour l'Europe, propose notamment, à travers le développement de nouveaux systèmes d'informations, "*des décisions transparentes*", "*une visibilité et un accès des données pour tous les acteurs du système*" grâce à la collecte précise des données sur la capacité et la demande, *etc.* C'est aux compagnies aériennes, notamment, que le processus deviendra plus transparent. Toutes ces questions méritent sans doute qu'on s'y arrête[80].

Dans le cadre nécessairement limité d'une première recherche, nous avons choisi d'ancrer notre réflexion sur la transparence dans un "objet" qui fasse sens pour l'organisation, et qui s'inscrive dans des enjeux actuels importants, sans se limiter à un intérêt purement académique. Dans le contexte actuel, les questions liées à la visibilité des incidents apparaissent particulièrement cruciales. Ces questions trouvent, en outre, une résonance accrue avec le développement d'un "*outil de surveillance automatique de la sécurité*" qui permet la détection automatique de certains incidents.

Le contexte

Le contexte actuel permet de circonscrire davantage notre questionnement, en l'articulant avec les enjeux qui se dessinent.

Depuis quelques années, le contexte institutionnel du contrôle de la navigation aérienne se développe, avec la création de la PRC (Performance Review Unit) et de la PRU[81] (Performance Review Commission) d'une part, et de la SRC et SRU d'autre part. La PRC est chargée d'analyser les performances du système ATM (gestion du trafic aérien) en Europe, en développant des indicateurs, et en proposant des mesures d'amélioration, sans toutefois avoir de pouvoir réglementaire. Créée en 1998, la SRC (commission de réglementation de la sécurité), a pour rôle d'établir, d'harmoniser et de coordonner les approches dans le domaine de la sécurité. Elle est appuyée par la SRU, (Safety Regulation Unit) qui réalise différents travaux utiles aux objectifs de la SRC.

En outre, un processus de séparation du fournisseur de service de navigation aérienne et de l'autorité réglementaire est en marche, avec, dans certains cas, la privatisation du service du contrôle de la navigation aérienne.

Dans ce contexte de changement, des travaux cherchent à faire le bilan de la sécurité du point de vue du rôle du contrôle aérien. En effet, si on dispose d'assez nombreuses données côté compagnies aériennes, c'est plutôt l'inverse pour les incidents liés au contrôle aérien. Le rapport Européen sur les performances de l'ATM en 1998, établit qu'il "*existe des différences significatives, au sein de la zone ECAC, dans la portée, la profondeur, la cohérence et la disponibilité des données de sécurité ATM*[82]". De plus, "*il a été trouvé qu'il n'existait que des données limitées pour les incidents liés à l'ATM, autres qu'AIRPROX. Par exemple, il y a très peu de données sur les "quasi CFIT*[83]*" (Control Flight Into Terrain) ou les incursions de piste*". De plus, les données sont collectées, classées, analysées, selon

---

[80] Ce pourrait être d'ailleurs l'objet d'un prolongement dans une thèse que de réfléchir à d'autres aspects de la transparence, portant sur d'autres "objets" , et d'analyser si la transparence est une valeur transversale dans une organisation ou si elle prend des sens différents en fonction de l'objet auquel elle se rapporte.

[81] *The Performance Review Commission (PRC) was established in 1998 by the Commission of EUROCONTROL, in accordance with the ECAC Institutional Strategy (1997). One objective in this Strategy is "to introduce strong, transparent and independent performance review and target setting to facilitate more effective management of the European ATM system, encourage mutual accountability for system performance and provide a better basis for investment analyses and, with reference to existing practice, provide guidelines to States on economic regulation to assist them in carrying out their responsibilities*. Site Web Eurocnotrol.

82 ESARR 2 : "*Notification et analyse des évènements liés à la sécurité dans le domaine de l'ATM*'.

83 "Accident in which an aircraft, under the control of the crew is flown into terrain, or water, with no prior awareness on the part of the crew of the impending accident. CFIT represent 50% of aircraft accident fatalities worldwide. Source : Eurocontrol Safety letter, EATMP Safety Group.

des critères très différents selon les pays[84]. La réglementation ESSAR 2 établit une exigence réglementaire de notification et d'analyse des évènements liés à la sécurité dans le domaine ATM, et un document annexe[85] définit les critères d'un "report obligatoire" d'incidents et d'un report "volontaire". La réglementation ESSAR 3[86] recommande la mise en place de "Safety Management Systems", c'est à dire le développement de services dédiés à la gestion de la sécurité au sein de chaque fournisseur de service de navigation aérienne national[87].

La mise en place de la SRC ne va pas sans poser sans poser quelques tiraillements, il s'agit entre autres, de bâtir une transparence des organisations de service de contrôle de la navigation aérienne vers une institution réglementaire européenne, quant aux incidents, et bien sûr, tout ceci est nouveau.

Une personne de la SRU nous explique : "*L'Annexe 13 de l'OACI oblige les états à rapporter les incidents sérieux. On l'a écrit et les gens sont choqués : la plupart des états ne respectent pas cette règle*". Elle continue : "*Le regard est négatif, très négatif, pour le moment, on est la police. Il y a une relation de confiance à bâtir. AIRBUS aujourd'hui est le premier à dire qu'ils ont besoin du SFACT ou des JAA, que cela leur rend service pour la sécurité, que cela fait un regard en plus pour la sécurité, ils ne remettent plus en cause la nécessité d'un organisme de certification… Cette fonction-là est essentielle si elle est bien faite, après il faut regarder le fond des dossiers et non la forme, c'est la maturité du métier aussi*".

Quelle visibilité des incidents ?

Il existe en fait de nombreux moyens de connaître les incidents[88], certains sont humains, d'autres techniques, d'autres enfin sont "mixtes" : c'est un système qui détecte l'événement, qui restera connu des seuls humains, pilotes ou contrôleurs, à moins que ceux ci ne reportent l'incident.

Du côté humain, pour les pilotes on trouve : les AIRPROX déposés par les pilotes, les Air Safety Reports. L'AIRPROX a un caractère de "plainte" à l'égard du service de contrôle (le pilote considère que la sécurité a été mise à mal), alors que l'ASR est plus anodin.

Toujours côté humain, les incidents peuvent être aussi détectés par les contrôleurs. Certaines pertes de séparation, cependant, ne sont pas visibles[89]. De plus, on trouve à l'heure actuelle, des pratiques de report des incidents très différentes selon les pays. Des positions extrêmes existent : dans certains pays, il est normal et encouragé de reporter un incident, et des procédures précises sont définies; dans d'autres pays, les contrôleurs peuvent être sanctionnés en cas d'incident, et bien sûr, les incidents ne sont pas reportés par les contrôleurs. Enfin, entre les deux, des pays ne sont pas punitifs, mais n'organisent pas non plus le report d'incidents, et seuls les AIRPROX sont traités. Le document Eurocontrol cherche justement à harmoniser les pratiques quant à ce qu'il est obligatoire de reporter, et ce qu'on peut reporter volontairement, le tout en l'absence de sanctions pour le contrôleur.

Les incidents détectés par des moyens techniques se réfèrent à la norme. Côté avion, c'est le cas des programmes FOQA, déjà évoqués dans le chapitre 3, qui permettent l'enregistrement automatique d'incidents définis par un écart de paramètres à une normèr aOQA, déjàsnt9(u)2is1.0121 .3(s)-1-4.4(i(o)déj)681T(

Entre les deux, on trouve des incidents qui sont détectés par des systèmes, et qui peuvent être, en outre, reportés par les pilotes ou les contrôleurs.
Du côté avion, c'est le cas du TCAS. Ce système embarqué donne un avis de trafic, et dans les cas plus sérieux, un avis de résolution (RA) dans lequel il donne une manœuvre d'évitement à effectuer par le pilote. La plupart des compagnies rendent obligatoire le report d'un évènement TCAS.
Du côté contrôle, c'est le cas du filet de sauvegarde : il clignote lorsque ses calculs d'anticipation de la trajectoire indiquent que la norme de séparation risque de ne plus être respectée. Tous les services de contrôle aérien ne formalisent pas, pour le contrôleur, l'obligation de reporter cet événement.

Il existe donc des outils techniques et humains qui scrutent le système : ce sont des outils d'une forme d'auto-transparence dans le sens où on l'a évoqué tout à l'heure. Ce qu'il faut garder à l'esprit, c'est la diversité recouverte par le terme "incident". Ces outils techniques et les humains détectent des évènements qui se recouvrent, mais pas totalement. Un humain peut percevoir comme un incident un événement non détecté par un système, et un évènement détecté par un système peut être considéré par un humain comme non "risqué" : l'humain a des éléments de contexte, un jugement, une appréhension globale du risque. L'outil détecte des évènements qui sont hors des capacités perceptives de l'humain, c'est en tout cas juste pour l'analyse des vols.

Il existe à la fois des évènements qui sont multidétectés : par exemple une perte de séparation dans un centre en route peut être : détectée par le TCAS dans l'avion, détectée par le filet de sauvegarde, reportée par le pilote dans sa compagnie, et par le contrôleur… mais il existe aussi (structurellement) des points aveugles : une incursion de piste par exemple, peut rester ignorée du pilote, le contrôleur peut s'en rendre compte mais ne pas être amené, ou ne pas souhaiter, pour de multiples raisons, le reporter. Même si les mécanismes sont différents, la notion de secret structurel proposée par Vaughan trouve ici aussi tout son sens[90].

On a donc un système dans lequel, pour prendre une métaphore un peu facile quand on parle de transparence, il y a à la fois, des évènements qui sont "sous le feu de projecteurs croisés" et des évènements qui sont "dans la pénombre la plus complète".

Un frein structurel : la culture punitive

En ce qui concerne le report volontaire d'incidents, un frein concerne une culture "punitive", qui, dans certains pays associe à l'incident une forme ou une autre de sanction pour le ou les contrôleurs impliqués.

C'était le cas au Danemark par exemple, jusqu'à cette année, la sanction étant essentiellement financière. La loi vient d'être modifiée, sous la Tc029 Tc□la

entraînement de rattrapage semble avoir un caractère de sanction, du moins est-il vécu de cette façon par les contrôleurs.

5.3. Un outil de surveillance de la sécurité : ASMT Automatic Safety Monitoring Tool

5.3.1. Description et bref historique de l'outil

Eurocontrol développe dans le cadre de ses activités liées à la sécurité un "outil de surveillance automatique de la sécurité" (ASMT). C'est aussi un outil d'aide au dépouillement et à l'analyse des incidents grâce à des fonctions de "rejeu" de la situation radar. Cet outil peut permettre plusieurs types de détection : dans un premier temps, il permet l'enregistrement des pertes de séparation, dès lors que la norme de séparation du centre a été enfreinte par deux avions, cette valeur pouvant bien sûr être paramétrée localement. Les autres fonctions prévues sont : la détection des "level bust", (c'est-à-dire toute déviation de plus de 300 pieds d'une clairance ATC), la pénétration de zones prédéfinies (par exemple de zones militaires), l'enregistrement automatique de reports des ACAS par liaison numérique, l'enregistrement automatique en dessous d'un niveau de vol minimum (type MSAW).

L'historique de ce nouvel outil mérite d'être rappelé ici. Se présentant souvent comme un pionnier dans le domaine de la sécurité, le NATS (fournisseur de services de contrôle aérien anglais) a développé le SMF (Safety Monitoring Function) voici plusieurs années. La petite histoire veut que ce soit le directeur du programme EATCHIP lui-même, qui, après démonstration du fonctionnement de cet outil, aurait demandé le développement de ce concept à Eurocontrol. Une solution initiale aurait consisté à reprendre l'outil informatique développé par le NATS puis à le paramétrer pour les besoins de Maastricht. Après de nombreuses tergiversations liées notamment à l'acceptabilité d'un tel outil par les contrôleurs, il a décidé de développer un outil "maison", ce qui a été confié au Centre Expérimental de Brétigny. Il fut décidé également que le centre de contrôle aérien pilote pour l'installation serait le centre de Maastricht. Ensuite, Eurocontrol proposera la mise en place d'ASMT dans les différents états membres.

Dès la phase de spécification de l'outil au centre expérimental d'Eurocontrol, il a été décidé de se démarquer de l'utilisation du SMF par le NATS. En effet, une perte de séparation détectée par le SMF conduit à une enquête rapide de la cellule en charge de la sécurité, puis peut conduire à la suspension de ses fonctions le contrôleur responsable de l'incident, le temps qu'une enquête plus approfondie soit effectuée. Des incidents répétées chez la même personne semblent pouvoir mener, dans certains cas, à la suspension de la licence de contrôle (quoiqu'il soit difficile d'obtenir des informations détaillées sur le processus et l'ampleur exacte de cette procédure). A l'inverse, Eurocontrol souhaite prôner, avec ASMT, une "non punitive culture" et insister sur l'utilisation de la connaissance des incidents dans une perspective d'analyse et de Retour d'expérience, afin d'améliorer la sécurité globale. Comment deux objets techniques aux fonctionnalités générales relativement similaires peuvent-ils prétendre à des visées opposées ? Comme le rappelle Sophie Poirot-Delpech dans sa "Biographie du CAUTRA", : "*Un projet n'est jamais purement technique et les dimensions humaines (politiques par exemple) sont constitutives de sa réalisation. Un objet technique (…) reste ouvert à des captures, des appropriations souvent imprévisibles. La socialisation d'un projet fait partie de sa définition, de sa constitution : il est impossible d'arrêter la définition d'un projet technique à ce qu'on a voulu mettre dedans*".

C'est pourquoi les procédures qui vont être définies avec l'outil, procédures qui définissent l'usage de l'outil, les spécifications mêmes de l'outil pour certains aspects, le réseau d'acteurs qui l'entourent : qui voit quoi ? qui a accès à quoi ? que fait-on de l'information ? *etc.*, vont réellement définir le rôle de cet outil.

Une première étude menée dans le cadre d'une mission de conseil pour Eurocontrol, avait permis d'identifier quelques caractéristiques particulièrement prégnantes de l'ASMT :

- l'ASMT est un outil lié à la transparence : il met à jour des évènements (pertes de séparation) qui, sans ASMT, peuvent rester connus des seuls contrôleurs impliqués, en ce sens il constitue la perte d'une forme d'intimité professionnelle (la possibilité de ne pas révéler ses erreurs, ratés, ayant occasionner une perte de séparation)
- dans un contexte de mise en place d'une autorité de régulation, cette transparence ne concerne pas seulement les contrôleurs vis-à-vis du management, mais aussi le management vis-à-vis de l'autorité de réglementation, les services de contrôle aériens vis-à-vis des compagnies aériennes clientes, *etc.*
- autour de l'ASMT se cristallisent les questions liées au sens de la sécurité et des "évènements sécurité" (symbolique de l'incident dans un monde où les accidents sont rares, rôles des différents acteurs dans la sécurité, rôles des contrôleurs dans cette sécurité aérienne avec toute l'ambivalence de la notion de responsabilité, à la fois poids insupportable et source de fierté, revendication).

5.3.2. L'installation sur site pilote : tensions et questions

L'installation sur site pilote, à Maastricht, ne s'est pas faite sans tensions.

Sécurité ou séparation ?

Un débat sur l'acronyme, d'abord. En quoi cet outil surveille-t-il la sécurité ? que veut dire d'ailleurs surveiller la sécurité ? Dans sa première version, ASMT ne détecte que les pertes de séparation.

"ASMT n'est pas un outil de surveillance de la *sécurité*, c'est un outil de surveillance des *séparations*"… dit une contrôleuse[92] qui fait partie du groupe de définition des procédures associées à l'outil.

Or, qu'est-ce qu'une perte de séparation ? qu'est-ce que cela signifie du point de vue de la sécurité ? et que fait-on de cet incident ? Autant de questions qui sont restées sans réponse car il n'y avait pas eu de réflexion très poussée sur la relation entre perte de séparation et sécurité.

Dès lors, les tiraillements autour d'ASMT sont autant de révélateurs de compréhensions et visions de la sécurité, différentes parfois entre les contrôleurs eux mêmes, mais aussi, de façon plus attendue, entre contrôleurs et encadrement, régulateur, *etc.* Ces compréhensions différentes n'ont quasiment jamais eu l'occasion d'être débattues entre les acteurs, et tout ceci reste implicite. En parlant avec les différents acteurs, on retrouve par exemple l'opposition entre un modèle trop simple pour être juste (plus la séparation est petite, plus la sécurité a été "mise en danger") qui prédomine souvent côté encadrement, et un modèle plus qualitatif qui s'apparenterait plus au concept de "*maîtrise de la situation*" de René Amalberti.[93]

Pour l'expliquer un peu vite : certaines pertes de séparations sont maîtrisées (elles correspondent à des séparations à vue, et le contrôleur, en ce cas, informe chacun des avions en lui signalant la présence de l'autre). Dans ce cas l'ASMT se déclenche : il ne peut pas "savoir" que la séparation est maîtrisée. Deuxièmement, la configuration des secteurs à Maastricht implique que les croisements, si on veut être capacitif, se font "juste à la limite" de la norme de séparation. Une petite perte de séparation ne correspond donc pas à un véritable "risque" mais seulement à un peu de malchance dans l'évaluation. Or, ASMT transforme soudainement ces données dans une logique binaire : 5,1 : pas de risque, 4,9 : risque. Seul le contexte (donné par le contrôleur) peut éclairer sur la signification à donner à chaque événement. Enfin, il existe des incidents qui ne vont pas se traduire en pertes de

[92] *For us, ASMT is not a safety monitoring tool, it is a separation monitoring tool.*

[93] La maîtrise de la situation porte sur un résultat acceptable sur l'objectif de travail, et pas sur le jugement évènementiel instantané. *Approches ergonomiques des erreurs et du risque*. René Amalberti. Colloque CNRS Risques collectifs et situations de crise. Février 2000.

séparation, mais qui sont vécus comme tels[94], par exemple, un avion complètement oublié, mais dans un contexte où cette erreur n'a pas eu de conséquence, une coordination ratée mais rattrapée, *etc.*
Un superviseur rapporte les réticences d'un contrôleur à l'égard d'ASMT : "*bon alors, je fais une petite perte de séparation, mais rien de grave, je maîtrise , et alors là, avec ASMT, on va venir me voir et me dire : "tu t 'es trompé ! tu as fait une erreur !" et on va m'embêter là dessus. Mais deux jours avant je me serais fait une vraie frousse, mais pas de perte de séparation, et là il n'aura rien vu, l'ASMT : c'est pas juste*".

Ce qui n'est pas sans rappeler ce qui a été dit dans le chapitre 3 sur l'acceptabilité d'une forme de transparence par un professionnel dans son travail : ici, le qualificatif *juste* qui est donné par le contrôleur paraît particulièrement fort, il rappelle que la transparence n'est acceptable que si on peut se mettre d'accord sur le sens de ce qui est révélé.

Ne pas voir "plus" que le contrôleur…

La mise en place d'un outil est souvent l'occasion de tensions entre une vision d'ingénieur et une vision d'utilisateur. L'ASMT en fournit un exemple frappant. En résumant un peu les choses, la vision des ingénieurs est qu'il fallait mesurer les *vraies* pertes de séparation. En conséquence, il fallait utiliser, comme données d'entrée radar, les pistes brutes des avions. Les opérationnels se sont farouchement opposés à cette solution. Il fallait, de leur point de vue, utiliser les données radar lissées, les mêmes en fait qui servent à présenter les plots radar sur leur écran. Or ces données sont moins *justes*, puisque le Système de Traitement Radar opère la visualisation des plots en termes probabilistes. Ce qui veut dire qu'en choisissant la solution des ingénieurs, l'ASMT aurait pu détecter des pertes de séparation non détectées (car non détectables) par le contrôleur. Il est clair également qu'il ne s'agissait pas de reprocher au contrôleur, lors de l'analyse de l'incident, de ne pas avoir détecté les quelques séparations *invisibles* par le contrôleur sur son écran radar ! Les ingénieurs souhaitaient surtout se doter d'un outil qui soit le plus *objectif* possible, alors que les opérationnels se sont d'emblée méfiés d'un outil qui en aurait su plus qu'eux. C'est cette vision qui a prévalu dans les spécifications finales de l'outil[95].

Surveillance de la perte de séparation ou surveillance du contrôleur ?

Un deuxième débat concerne l'utilisation de l'outil. Avec ASMT, une des utilisations premières (ce qu'on a appelé "la procédure initiale", consiste à mesurer automatiquement des pertes de séparations réelles. Dans la plupart des cas, une alerte ASMT a déjà donné lieu au déclenchement d'un filet de sauvegarde sur la position du contrôleur. Or, le contrôleur est censé reporter l'incident en cas de filet de sauvegarde. C'est pourquoi, l'ASMT se voit qualifier par certains contrôleurs de "snitching tool". Très vite également, la référence à Orwell est entendue : ASMT est une sorte de "Big Brother" qui surveille les erreurs du contrôleur.

Sophie Poirot-Delpech, dans sa "*Biographie du CAUTRA*", avait analysé la mise en place de PATATRAC, l'ancêtre d'OPERA[96], c'est à dire un système qui comme ASMT, enregistre automatiquement les pertes de séparation. Les réticences des contrôleurs, dans le cas français, venaient plutôt d'une crainte de voir l'outil utilisé comme système d'évaluation des équipes et des contrôleurs, ces derniers perdant un peu de leur fameuse opacité de fonctionnement vis-à-vis de la hiérarchie. Finalement PATATRAC, puis OPERA seront utilisés en France pour l'analyse individuelle d'incidents, dans une perspective radicalement non punitive.

---

[94] La limite entre ce qui est un incident et ce qui ne l'est pas est une question complexe qui dépend du modèle de sécurité que l'on utilise, problème n'est pas abordé dans cette recherche. On se focalise ici sur la perception du risque par le contrôleur, en faisant le postulat implicite que son jugement a une importance centrale.

[95] Il semble pourtant, que la solution *ingénieur* aurait pu permettre de développer une utilisation d'ASMT supplémentaire centrée sur le calibrage de la confiance des contrôleurs envers leur outil radar. (L'avion n'est pas exactement là où il est affiché, il est simplement probablement là, à l'intérieur d'un cercle prédéfini).

[96] OPERA et l'ASMT reposent sur un principe similaire : l'enregistrement automatique des pertes de séparations réglementaires. Mais OPERA utilise les données du filet de sauvegarde, qui extrapole les trajectoires des avions, tandis qu'ASMT reçoit ses données du Système de traitement Radar, et enregistre ainsi les pertes de séparations réelles. De plus, OPERA se cantonne aux pertes de séparation F.D.S, tandis qu'ASMT, on l'a vu, peut enregistrer d'autres évènements (level busts, par exemple). (Que les spécialistes me pardonnent cette description sommaire).

A Maastricht, les procédures d'utilisation initiales de l'outil se centraient bien sur une détection des pertes de séparation de 4,9 NM en séparation horizontale. Si l'outil se présentait comme un "complément au report d'incidents fait par les contrôleurs", il pouvait être ressenti, à juste titre, comme une "forte incitation" à reporter tout incident lié à un filet de sauvegarde. De plus, dans un contexte dans lequel l'accent est mis depuis des années sur la capacité, ASMT a été ressenti comme une forme de "double bind" au sens de Laing : il faut à la fois faire passer toujours plus d'avions *et* accepter désormais de se faire attraper à la moindre perte de séparation !

Enfin, il semble que l'outil ait été introduit au départ en faisant état d'une *obligation réglementaire,* alors que l'obligation n'existait pas, et n'est d'ailleurs pas prévue (les futurs documents réglementaires font état d'une possibilité d'utiliser ASMT dans l'éventail des moyens de collecte d'évènements, mais en aucun cas d'une obligation). Après quelques mois d'atermoiements et de test pré-opérationnel, l'organisation professionnelle des contrôleurs, l'EGATS s'investit davantage dans les procédures liées à l'outil ASMT, et élabore des propositions concrètes pour une utilisation de l'outil sensiblement différente.

La paix retrouvée ? : une histoire d'appropriation

Simondon[97] a forgé la notion de marge d'indétermination pour rendre compte de ce qui restait "ouvert" dans l'utilisation de tout objet technique. C'est cette marge qui va rendre possible l'appropriation par les utilisateurs : un exemple de ce processus d'appropriation est fourni par Caroline Moricot[98] dans sa recherche sur l'automatisation des avions, et la façon dont les pilotes vont peu à peu faire du glass cockpit "leur" système.

L'appropriation, n'est pas un simple processus d'adaptation des utilisateurs à leur outil : c'est aussi un "processus créatif dans lequel les personnes investissent leur énergie et leurs idées". Ce processus va permettre de modeler l'utilisation d'un outil, et d'arriver parfois à une utilisation qui n'avait pas été anticipée au moment de la conception de l'outil.

En reprenant la typologie des objets techniques présentée dans le chapitre 3, ASMT pourrait être lié à :

- ➔ quelque chose qu'un sujet ou collectif souhaite cacher, ou plus communément ne souhaite pas systématiquement révéler ( ). Exemple : j'ai un incident et ASMT enregistre la perte de séparation dont je ne voulais pas parler. Il faut noter qu'il existe de nombreux freins au report d'incident même dans une culture non punitive (l'envie d'oublier la peur qu'on a eu, l'impression d'inutilité, le désintérêt pour la "paperasserie", cf. chapitre suivant.

- ➔ quelque chose dont un sujet ou un collectif a une conscience diffuse mais n'a pas l'occasion de l'objectiver, et l'objet technique va alors simplement montrer ce que "tout le monde savait intuitivement déjà" ( ). Par exemple, (voir plus loin) ASMT montre que les contrôleurs descendent en dessous des 5 MN en utilisant le plus souvent la procédure VMC alors qu'elle n'est pas autorisée dans l'espace de Masstricht : tout le monde s'en doutait, mais des données objectives l'attestent, l'enregistrent : pour l'organisation (et pour les managers, le régulateur, *etc.*,*…* ce n'est sûrement pas la même chose). Un exemple côté avion : l'analyse des vols a montré des dépassements nombreux de vitesse supérieurs à 250 kts dans les espaces de classe D[99];

- ➔ soit l'objet technique montre quelque chose dont un sujet ou un collectif seuls ne pouvaient appréhender le sens, parce que l'objet technique est capable de rassembler/synthétiser des données et de coordonner des données disparates et d'origine différente. ( )

[97] Gilbert Simondon. *Du mode d'existence des objets techniques*. Aubier, Philosophie. 2001.
[98] Caroline Moricot. *Des avions et des hommes*.Septentrion. 1997.
[99] Bulletin Décembre 2000 de la sécurité aérienne, DNA.

En se centrant sur l'identification individuelle d'incidents, l'ASMT pouvait être ressenti par les contrôleurs comme une forme d'espionnage. On verra dans le paragraphe suivant que cette surveillance est peut être acceptable dans certaines conditions.
L'EGATS a très vite proposé une utilisation qui ferait d'ASMT un outil pour dévoiler ou révéler des problèmes, en s'intéressant moins à l'occurrence d'incidents individuels, et plus à des tendances. Dans ce cas, l'outil permet plutôt de se poser des questions.

Nous avons vu qu'autour de l'objet technique ASMT, objet qui peut dévoiler/révéler/espionner, les acteurs ont d'ores et déjà développé des stratégies qui tournent autour de la question de la visibilité/dissimulation mais aussi et surtout autour du sens que l'on veut donner à l'information sur les pertes de séparation, sens qui s'élabore sur les représentations de la sécurité et qui va aussi modifier les représentations de la sécurité. On voit aussi tout de suite comment l'introduction même d'un objet censé mesurer la sécurité va d'emblée modifier la perception que les acteurs se font de la sécurité qui vont peut être aussitôt mettre en place, consciemment ou inconsciemment, une régulation de leurs conduites. Bien sûr, *tout le monde* était conscient que les contrôleurs utilisaient dans l'espace de Maastricht la séparation à vue (VMC) alors que celle ci n'est pas autorisée. *Tout le monde* savait également que les contrôleurs, afin d'écouler un des trafics les plus denses d'Europe, étaient amenés à descendre régulièrement légèrement au-dessous de la norme : mais le *savoir* est une chose, et le voir affiché jour après jour sur la base d'un outil qui objective ces pertes de séparations en est une autre. Dans ce cas, l'objet technique supporte, renforce, "réifie" le sentiment que les pertes de séparations existent, et qu'elles ne sont pas obligatoirement à interpréter comme des incidents.

5.3.3. Le contrôleur et l'intimité professionnelle

La définition de procédures liées à l'utilisation de cet outil et fait l'objet de nombreuses discussions et négociations qui ont fini par se stabiliser, de façon parfois sensiblement différente de ce qui était prévu au départ. Ainsi, il n'était pas prévu d'afficher sur l'écran radar du contrôleur un signal l'avertissant qu'une alarme ASMT avait été déclenchée. D'autre part, la procédure initiale prévoyait que l'alarme ASMT soit affichée sur l'écran du poste du superviseur, qui pouvait ainsi examiner aussitôt l'incident en "rejouant" la visualisation de l'image radar.

Quelques évolutions ont toutefois eu lieu : d'abord, le contrôleur a une petite "alarme" qui lui indique que l'ASMT a enregistré un "événement sécurité", selon le terme consacré. Ensuite, l'information ASMT est envoyée sur le poste de superviseur de la salle, mais ce poste était éteint au moment de notre visite. Les superviseurs ont demandé que l'alarme ASMT soit envoyée par réseau sur le poste informatique de leur bureau, bureau qui se situe hors de la salle de contrôle. Le superviseur nous a emmené dans son bureau, soigneusement fermé la porte, tapé son mot de passe et enfin montré les incidents de la journée, y compris ceux qui arrivaient en temps réel sur son écran. Il nous a expliqué que le poste de superviseur dans la salle de contrôle était trop visible de tous : "*mettez vous à leur place, hein, vous n'aimeriez pas qu'on voit… qu'on vous regarde, que si vous avez fait une erreur, tout le monde puisse le voir…*".

En miroir de cet "outil de la transparence" , le superviseur réintroduit ce qui nous semble être de l'ordre, non de l'opacité mais plutôt de *l'intimité* : il ne s'agit pas tant de cacher ce qui s'est passé que de protéger le contrôleur d'une intrusion. Ou plus précisément de ce qui pourrait être vécu par le contrôleur comme une intrusion, ou de ce que le superviseur (un ancien contrôleur devenu un manager) considère comme une intrusion vis-à-vis de ses "ouailles". Plus tard (notre superviseur a insisté sur le "plus tard" : on ne se précipite pas sur la position en demandant ce qui s'est passé…), le superviseur ira en salle voir le contrôleur à la fréquence. Il lui proposera de revoir son incident (ce que le contrôleur accepte, voir demande spontanément semble-t-il, dans la majorité des cas), et le cas

5.4. La transparence comme fin en soi ?

ASMT s'inscrit bien dans une visée d'*auto-transparence* caractéristique de la Modernité et des Macro Systèmes Techniques, comme on l'a vu dans le chapitre 2 et 3. ASMT n'est pas étranger à une forme de culte de l'information : l'information comme paradigme dominant, la confusion dans le langage entre information et vérité, le glissement qui s'opère entre vérité, et transparence ont déjà été mentionnés comme caractéristiques de la modernité par Philippe Breton au début du chapitre 2.

ASMT n'est bien sûr pas étranger à ce culte, et il en est ainsi de beaucoup de réflexions sur la collecte d'incidents, qu'elle soit automatisée ou non. Il s'agit d'éclairer, voire, pour reprendre notre métaphore facile, de multiplier les feux croisés des projecteurs sur les incidents. Mais cette ferveur dans la collecte n'a parfois d'égal que la discrétion sur le *sens* donné à cette information, et sur son utilisation effective. On peut bien stigmatiser alors, dans certains cas, l'idée d'une transparence comme fin un soi, d'une "frénésie" de transparence comme le disait Guy Carcassonne (chapitre 2) dans une analyse à la portée plus générale.

A la question : "*et que faîtes vous de ces données (sur les incidents) ?*" , un responsable sécurité répond sans sourire : "*eh bien, des bilans, toutes sortes de bilans*", "*Certes, mais… avec ces bilans ?*" "*eh bien, des bilans généraux, des rapports de synthèse*"…

Dans le chapitre suivant, on verra, à travers l'analyse de plusieurs organisations ATM Européennes, que la notion de transparence prend un sens tout à fait différent suivant le pays et l'organisation. Dans chacun de ces contextes, ASMT (que son existence soit évoquée ou que l'organisation ait déjà planifié son installation) prend une dimension différente.

Chapitre 6.
Quelques organisations ATM à l'épreuve de la transparence

Il y a un exemple précis que j'ai appris par Internet, c'est tout à fait amusant, il y a des sites, un truc français assez bien fait : radio cockpit, c'est comme ça que j'ai appris un incident relativement grave

Un responsable sécurité

6.1. Introduction

Dans ce chapitre, plusieurs organisations de contrôle de la navigation aérienne sont examinées quant au traitement des incidents dus au contrôle. Il s'agit d'une première approche permettant de poser quelques réflexions, et non d'une véritable analyse comparative. Les pays examinés sont : la France, la Slovaquie, le Danemark, l'Italie, la Suède.

Cette partie ne prétend pas faire un état de l'art exhaustif des pratiques liées à l'analyse d'incidents, ce qui constituerait une étude à elle seule. Le fil conducteur des questions sur la transparence qui ont été posées jusqu'à présent sert à délimiter ce qui est traité. C'est à dire, pour rappel : l'*auto-transparence* d'une organisation (comment cette organisation se connaît elle-même, et identifie ses risques), et les limites structurelles de ce processus, la transparence d'une organisation vis-à-vis de l'extérieur, et le sens donné par un professionnel à la transparence qui lui est demandée.

Une autre limite de ce chapitre doit être gardée à l'esprit : dans chacun des pays, un seul centre de contrôle aérien a été visité. Or, on sait qu'à l'intérieur d'un même pays, les différents centres de contrôle aérien peuvent être très différents. C'est bien le pays qui est mentionné, et non tel ou tel centre, parce qu'à chaque fois les "quartiers généraux" ont été également approchés, mais les descriptions doivent être lues comme des embryons d'ethnographie et d'analyse, pas davantage.

Dans chaque pays, nous avons rencontré le responsable sécurité (Safety Manager), et d'autres personnes ayant un rôle dans la sécurité, une personne au moins côté autorité de réglementation. Nous avons visité un centre de contrôle en route au moins, puis une approche et une tour lorsque c'était possible. A chaque fois, nous avons rencontré une ou plusieurs personnes en charge de l'analyse d'incidents, le responsable opérationnel du centre, éventuellement d'autres personnes de la hiérarchie, notamment en charge des aspects "Facteurs Humains" ou TRM, et enfin, bien sûr, des contrôleurs. Tout ceci étant bien entendu modulé par les disponibilités de chacun et les opportunités lors de notre visite. Nous avons rencontré également une personne de l'IFATCA et une de la "Safety Regulation Unit" d'Eurocontrol.

Afin de préserver l'anonymat des citations, nous mentionnons seulement la caractéristique "responsable sécurité", sans préciser s'il s'agit du "Safety Manager" au sens de la terminologie d'Eurocontrol, (car il n'y en a qu'un par pays !) ou de toute personne qui s'occupe de sécurité au sens large.

6.2. Quels sont les événements analysés ?

On a vu au chapitre précédent la diversité des moyens techniques et humains de collecter des événements, signaux, incidents. Le type même de ce qui est qualifié "intéressant à examiner" varie en fonction de la compréhension de la sécurité de chaque organisation. On retrouve là la notion de *sensemaking* de Weick : la sélection même de ce qu'il faut regarder n'a rien d'un *donné,* c'est une *construction de l'organisation*. On peut faire l'hypothèse, de plus, qu'il y a un renforcement du paradigme dominant, au sens où l'entend Henri Laroche[100] (le paradigme est déjà un facteur structurant des problèmes, il donne des grilles de lecture des problèmes) : plus on regarde un type de données que l'on considère intéressant du point de vue de la sécurité, plus on renforce le paradigme qui avait amené à sélectionner ce type de données). Pour être plus concret, plus on regarde les pertes de séparation, plus on renforce l'implicite qui nous a fait choisir les pertes de séparation comme évènement qui a du sens.

[100] Hervé Laroche. *Risque, Crise et problématique de la décision dans les organisations*. Séminaire Risques collectifs et situations de crises. 15 Novembre 1995.

Ensuite, au niveau purement quantitatif, plus on a de moyens, plus on collecte d'incidents, mais aussi, ce qui est moins trivial, plus on met en place des outils d'alarme (comme le FDS ou le TCAS) plus on "voit" de choses : on est bien alors dans le projet d'auto-transparence du Macro Système Technique dans lequel plus un système est bardé de dispositifs d'alarmes, plus il "énacte" au sens de Weick, d'incidents. D'où, peut être un paradoxe qui n'est qu'apparent : plus vous vous donnez de moyens d'être sûrs, plus vous voyez de défaillances.

C'est en ce sens qu'un responsable sécurité discute les chiffres qui sont affichés par le contrôle aérien français :

> *Quand même au niveau sécurité effectivement on pourrait dire qu'on en a trop d'Airprox, 800 alertes TCAS en 2000, 70.000 alertes F.D.S. dont tant de réelles c'est énorme. C'est énorme ? Non, on a différents gisements, d'investigations qui permettent de révéler ces informations ça c'est important aussi à prendre en compte. Le pays qui n'a pas le F.D.S, où l'activité n'est pas la même va dire, moi j'ai pas d'alerte, quelques TCAS, j'ai 18 Airprox, bon, je ne sais pas ce qu'il dit vraiment mais il faut être prudent quand on analyse les chiffres, c'est le rôle aussi un peu de la S.R.C mais ils le savent…*

Ensuite, les caractéristiques de la collecte vont dépendre d'éléments de l'organisation ATM (ses outils, la structure d'un service de gestion de la sécurité lorsqu'il existe, *etc.*), des compagnies aériennes (qui auront des pratiques de déclaration d'AIRPROX différentes) mais aussi d'éléments beaucoup plus macroscopiques tels que le caractère punitif ou non de la loi relative à la sanction des erreurs professionnelles dans chaque pays.

La tendance générale est la collecte de données focalisée sur les AIRPROX. Ce qui a été d'ailleurs identifié par le travail de synthèse fait par la SRC : "*il a été trouvé qu'il n'existait que des données limitées pour les incidents liés à l'ATM, autres qu'AIRPROX*".

, jusqu'à présent, l'analyse des incidents restait locale, et rattachée au directeur des opérations. Deux personnes étaient en charge de l'analyse d'incident. Les incidents analysés viennent essentiellement de réclamations des compagnies aériennes ou des militaires, et il y en a très peu.
Un changement d'organisation récent a permis la création d'un département chargé de la sécurité et la nomination d'un gestionnaire Sécurité : (Safety Management system et Safety manager selon les directives d'Eurocontrol). La situation est simple, puisqu'il n'y a pas ou quasiment pas d'Airprox.

> *Question : que pourriez vous dire de la sécurité dans votre pays ?*
> *Je dirais… (il rit) elle est absolue. Parce que nous n'avons eu aucune occurrence durant ces trois dernières années*[101]*.*
> *Rien ? Aucun Airprox ?*
> *Si, deux avec militaires, mais nous n'étions pas coupables.*

les analyses d'incidents sont effectuées par les cellules "Qualité de Service", mises en place depuis plusieurs années dans les CRNA, et plus récemment dans les Approches.

L'effort porte essentiellement sur l'analyse des AIRPROX déposés par les pilotes. Ce que regrette d'emblée une des personnes en charge de la sécurité :

> *Il n'y a pas que l'Airprox qui mérite l'attention aujourd'hui, on loupe énormément de REX en ne regardant que les pertes de séparation, c'est pas encore dans les esprits, l'idée c'est de parler d'incident significatif, le nom importe peu, le mieux, c'est de ne pas l'appeler AIRPROX pour permettre aux gens de ne pas penser uniquement pertes de séparation.*

[101] I would say it is (il rit) absolute, ABSOLUTE. Because we had no occurrences last 3 years.

Avec cette focalisation sur les Airprox, on est peut être dans un cas typique dans lequel il y a renforcement du paradigme dominant (le travail du contrôleur est de séparer les avions), au détriment d'une vision plus riche et plus complexe du travail des contrôleurs. Selon le même responsable, cette focalisation empêche parfois d'identifier les précurseurs d'accidents bien réels.

> *Si on regarde les accidents qu'il y a eu ces dernières années, ce n'est jamais lié à des pertes de séparation, mais sur ces autres choses on n'a rien, on n'a pas de précurseurs et on ne travaille pas assez…*

La France présente une spécificité, unique parmi les pays étudiés ici et, à notre connaissance, en Europe : un outil de recueil et d'exploitation hors ligne des alertes FDS, tandis qu'un processus de filtrage va permettre ensuite de sélectionner les "alertes réelles". Le filtrage s'opère en fonction… des moyens dont on dispose pour traiter les données.

> *Jusqu'à présent on parlait de H.N.R.N. (Hors Normes Réduites Nationales) pourquoi, parce qu'on s'est dit on va analyser tout ce qui passe en dessous des normes au départ, on s'est aperçu que c'est un travail énorme, on n'avait pas les moyens humains de le faire donc l'Administration a dit on ne va faire que les demi-normes, en dessous de la demi-norme, d'accord ce n'est pas tout mais c'est un échantillon suffisamment représentatif c'est pas la peine de tout faire pour avoir une idée des grandes causes, donc, parmi toutes les alertes en dessous des normes.*

Ces moyens évoluent, le filtrage de même :

> *Depuis le début de l'année, des centres nous ont dit on est capable de faire mieux, au niveau moyens techniques, moyens humains, on va passer au H.N 70. 70% de la norme. C'est à dire qu'actuellement depuis le 1er janvier 2001 sont analysées par l'homme finement, non plus les alertes qui sont en dessous des 50% de la norme mais celles qui sont en dessous de 70% ce qui veut dire 3,5 nautiques et 700 pieds ou 1400 pieds*

Y a-t-il redondance entre les moyens techniques et les moyens humains ? pas tant que ça, car le report spontané d'incidents par les contrôleurs n'est pas encore usité :

Quand on compare les alertes FDS CRNA par rapport aux Airprox CRNA, on s'aperçoit que très peu d'alertes réelles entre IFR/ IFR ont donné lieu à dépôt d'Airprox, d'une part. Aucune à un report contrôleur. Sur 80 alertes HNRN, c'est à dire en-dessous de la demi norme, environ, une dizaine de dépôt d'AIRPROX et zero report contrôleur. Un responsable sécurité.

non plus, le report d'incident sur initiative du contrôleur ne fait pas partie des pratiques, et la matière première est également constituée par les Airprox. Au centre de Rome, les Airprox sont analysés par le bureau de la sécurité, le formulaire est ensuite envoyé à un bureau national, qui peut décider dans certains de mener une analyse complémentaire.

Une grande attention semble être apportée à l'évaluation de l'incident en termes de risque[102]. La cellule locale et le bureau central font une évaluation séparée, puis comparent leurs résultats (cohérents dans la majorité des cas).
Tous les événements sont analysés, mais certains avec plus de "profondeur" que d'autres, non pas parce que la norme de séparation finale serait plus faible, mais parce qu'ils sont plus "intéressants".
Un analyste nous donne l'exemple d'un événement intéressant : il s'agit d'un incident avec une perte de séparation et une alerte TCAS (ce n'était donc pas si dangereux, nous dit-il) car deux avions avaient été "clairés" au même niveau.

[102] Il existe une évaluation du risque en 5 notes de A à E, un paragraphe traite précisément des débats nourris sur cette classification.

L'un des deux contrôleurs était un instructeur, et l'autre un contrôleur à l'entraînement. Il y avait beaucoup de trafic, ce qui semblait être une bonne situation pour l'entraînement. On a découvert que l'instructeur a forcé un peu, pas volontairement, mais il a forcé le contrôleur relevé à quitter sa place et à partir. Pour cette raison, ils n'ont pas eu toute l'information nécessaire à la relève, et en particulier, le contrôleur arrivant ne savait pas que l'avion venant du sud avait été clairé au même niveau que l'autre. Pourquoi ? Pourquoi a t-il accepté de quitter sa place avant le moment opportun ? Parce que l'arrivant est un instructeur, il a plus d'autorité… on essaie d'aller au delà des raisons du type : mauvaise clairance, tu as clairé un avion au mauvais niveau, mauvaise façon de travailler… Parce que si le premier contrôleur avait continué à travailler, il avait prévu, lui, de tourner l'autre avion à gauche, et c'était résolu.

on recueille comme toutes les autres organisations des Airprox, mais une caractéristique essentielle consiste en collecte largement basée sur le report spontané d'incidents par les contrôleurs eux mêmes[103]. L'idée générale étant qu'il vaut mieux "*reporter un incident sans intérêt que de laisser de côté un incident important*". L'organisation de la collecte est bien rodée avec des formulaires de DA (incident) : une centaine par an, de DI (n'importe quel problème qui a affecté le travail mais pas obligatoirement la sécurité). Les contrôleurs peuvent remplir et envoyer un formulaire, ou bien envoyer un formulaire électronique par Internet, (des ordinateurs sont disposés à plusieurs endroits, près de la salle de repos notamment). Environ 70% des incidents sont maintenant envoyés par ce moyen. Souvent, ils remplissent le formulaire avec l'aide de leur responsable opérationnel, ce qui est aussi une première occasion de discuter de l'incident.

Une partie des incidents est analysée localement, seule une petite partie est investiguée par les quartiers généraux. Les rapports des unités locales sont tous transmis aux quartiers généraux, pour information, mais seul un très petit nombre d'incidents fait l'objet d'un processus d'investigation, long et coûteux en ressources. Ce ne sont pas obligatoirement les Airprox qui font l'objet d'une investigation, ce n'est pas non plus le critère de perte de séparation, car la raison peut paraître trop évidente : jugement erroné sur la distance entre les deux avions.

Dans le centre de Malmö, le report d'incident est donc, globalement, très ancré dans les pratiques des contrôleurs. Il existe un consensus fort entre la hiérarchie et les contrôleurs sur le caractère normal, naturel, du report d'incident. Le discours est uniforme à tous les niveaux de l'organisation. Les raisons évoquées tiennent de l'éducation (*on nous enseigne cela dès notre formation initiale*), de la confiance, mais du sentiment, tout simplement, que c'est utile pour la sécurité, en termes de Retour d'expérience.

"*En Suède, il y a une atmosphère ouverte, on ne voit pas le report comme un problème, on a été éduqué à le faire, heureusement, on reçoit beaucoup de support quand on a un incident, des managers, et aussi des collègues, on n'a pas à avoir honte*"[104]. (Un jeune contrôleur)

Il existe également un groupe de six contrôleurs, qui sont opérationnels à plein temps, mais qui disposent d'une journée tous les deux mois pour exposer sur un thème de sécurité choisi.

Une seconde originalité consiste dans le "Event That You can Learn From". Mis en place depuis 10 mois, à l'initiative d'un psychologue qui les aide à analyser les incidents, c'est un nouveau type de report qui permet de signaler quelque chose en rapport avec la sécurité sans lui donner le caractère officiel du DA[105]. Il s'agit d'un report et d'un apprentissage qui reste local selon la formule : "traitement local, remède local".

---

[103] Dans leur étude concernant les "aspects moraux liés au report d'incidents", Marlene et Thomas ont comparé le Danemark et la Suède, qui s'opposent radicalement sur les pratiques de report : absence de report presque total comme on vient de le voir au Danemark, contre pratiques très rodées de report et d'analyse en Suède. Ils ont noté que la Loi sur l'aviation, similaire dans son caractère punitif à la Loi Danoise, a été abrogée en 1986.

[104] *In Sweden there is an open atmosphere, we don't see it as a problem to report, we have been taught to do that, hopefully we get a lot of support, when you have an incident, from the mangers, and also from your colleagues, there is nothing you have to be ashamed of.*

[105] Il est possible d'hésiter dans certains cas pour un contrôleur : DA ou ETYCLF ? un jeune contrôleur nous dit qu'en cas d'hésitation il demande à son superviseur, ou à la chef opérationnelle du Centre.

Il est à noter que les quartiers généraux du contrôle aérien Suédois ont d'abord vu avec un peu de méfiance la mise en place de ce qui apparaissait comme une entorse au "Tout Transparent" peu à peu acquis, avec la remontée de la plupart des incidents vers la base de données centralisée. Cependant, le principe d'un apprentissage local dans le centre de Malmö est désormais acquis, et semble répondre au souci d'un apprentissage local géré par les contrôleurs. En effet, le consultant qui a proposé la mise en place d'un tel système, souligne que "*la différence entre un événement lors duquel la séparation est enfreinte, et un événement lors duquel elle ne l'est pas, tient souvent tout simplement au facteur chance*". La classification dichotomique "incident/non incident" à partir de l'enfreinte d'une norme, renvoie à une compréhension trop simple de la sécurité : sécurité assurée tant que les avions sont séparés de la norme en vigueur, et sécurité soudain mise en danger dès lors que la barrière de la norme est franchie. La notion de ETYCLF renvoie pour sa part au jugement du contrôleur quant à une situation vécue comme *risquée*, même si la norme a été respectée.

6.3. Des freins au report d'incidents

S'il existe désormais un consensus concernant l'insuffisance des données Airprox, et la nécessité d'obtenir d'autres types d'informations, et ce de façon transversale aux différentes théories en ingénierie de la sécurité, il est alors utile d'examiner quelques freins au report d'incidents. Voici quelques exemples, qui ne prétendent pas non plus à l'exhaustivité.

6.3.1. Un frein juridique

S'il est un exemple qui montre l'impact de facteurs macroscopiques sur la transparence au sein d'une organisation, c 'est bien celui du Danemark.
En effet, jusqu'au 1er juillet 2001, la loi Danoise (Danish Aviation Law) permettait de soumettre à l'amende un contrôleur ayant eu un incident. La perte de la licence, et dans des cas extrêmes, la prison étaient également prévues. Le DATCA (organisation professionnelle Danoise du contrôle Aérien) a initié le changement de loi. Leur argumentaire s'est principalement construit sur le discours classique en ingénierie de la sécurité : la nécessité de connaître les incidents pour faire du retour d'expérience. En effet, très peu d'incidents étaient reportés, le report étant réservé aux cas pour lesquels "l'autre côté" (les pilotes pour les contrôleurs et vice versa) était à blâmer. Pendant longtemps, l'administration s'est félicité de ce qui apparaissait comme "une bonne sécurité" , attestée par le très petit nombre officiel d'incidents.

Il existe donc un lien indiscutable entre une loi punitive et la non transparence des incidents au sein de l'organisation, mais au delà du caractère concret de la punition, c'est le caractère absurde car inutile du point de vue de la sécurité qui est condamné par les contrôleurs

Le changement de Loi initié par l'organisation professionnelle des contrôleurs aériens Danois a été organisé en impliquant les différents media dans un débat public, (dont des émissions de télévision, de nombreux articles dans la Presse) qui mobilisa les citoyens Danois sur des réflexions de fond sur la justice et la sécurité des grands systèmes. Il est intéressant de souligner la façon dont le problème fut formulé par les contrôleurs Danois vis-à-vis du public : il ne fut pas défendu que la punition des personnes ayant provoqué un incident soit intrinsèquement inique, mais plutôt, que ce caractère punitif empêchait le report d'incident, donc le Retour d'expérience, l'apprentissage organisationnel, et par conséquent une meilleure sécurité.

" *Nous leur avons dit : vous devez choisir entre la justice et la sécurité*"

Les débats ont tourné autour du caractère juste ou non d'une mesure qui concernerait les contrôleurs et non d'autres professionnels, comme les médecins. Tandis que les partis politiques de Droite se focalisaient plus sur cette notion de justice, les partis de gauche s'intéressaient quant à eux davantage à la transparence des incidents vis-à-vis du public. Finalement la négociation se fit bien autour d'une garantie de transparence en échange de l'abolition du caractère punitif de la Loi. Il devient obligatoire,

pour les contrôleurs, de reporter leurs incidents[106], et ces incidents (sans l'identité des personnes impliquées) seront rendus publics en accord avec la "Freedom of Info Law". C'est en ce sens que la transparence qui se met en place au Danemark est une transparence négociée, nous montrant un exemple original d'un débat dans lequel des professionnels d'une organisation à haut risque et des citoyens ont pu débattre et trouver une solution.

En Italie, le changement est récent. Un responsable sécurité rappelle :

> *En 1992, je suis arrivé dans le département Sécurité, à cette époque, ça s'appelait le "bureau des enquêtes", depuis 2 ou 3 ans, on a changé le nom, on s'appelle : le bureau de la sécurité[107].* Un analyste d'incidents.

Même s'il est désormais stipulé que l'analyse des incidents n'a pas pour objet d'identifier un coupable, le changement est récent, et le report ne fait pas encore partie des pratiques.

En Slovaquie, le système prévoit une poursuite en justice pour des erreurs graves (si la séparation est enfreinte de plus de 70 % de la norme). Le dernier cas de poursuite d'un contrôleur remonte à 1984. Ces dernières années, aucune compagnie aérienne n'a déposé d'AIRPROX.

6.3.2. Un frein structurel

Si on ne peut que comprendre que le contrôleur cache ses incidents dans un pays qui sanctionne les erreurs, il existe d'autres raisons, et nous n'en explorons ici que quelques unes. D'abord, tout simplement le manque d'encouragement véritable à le faire, le manque de structures, de relais, de feed backs (pourquoi reporter s'il ne s'agit que de remplir un formulaire). Ensuite, mais ceci est lié, l'absence de sens donné à l'incident par l'organisation. Comme l'explique Helle Münsko, responsable de l'organisation professionnelle des contrôleurs au Danemark :

> *Il y avait aussi d'autres raisons de ne pas reporter[108]. L'une était la crainte d'avoir une amende, l'autre était de "perdre la face" , parce que la culture précédente impliquait : "on ne fait pas d'erreurs". Une autre explication est que le reporting n'était pas utilisé du tout de façon proactive. Je pense que nous aurions pu vivre avec les amendes (ou même pire) si seulement les rapports avaient été utilisés pour quelque chose d'autre tel qu'empêcher que la même chose ne se reproduise. Mais les rapports étaient utilisés seulement pour attribuer la faute à quelqu'un. Et un autre facteur était un processus d'investigation très long et très long. On a eu plusieurs exemples de cas, qui ont pris deux ans à investiguer : seulement pour conclure que le contrôleur était à blâmer et devait être mis à l'amende. Aucune autre recommandation. Ceci aussi fut une raison de ne pas reporter. C'est une épreuve très longue et très exigeante, pour n'importe quel être humain, que de vivre dans l'incertitude pendant si longtemps.*

---

[106] Ce qui permet de se conformer à une directive EUROCONTROL (ESSAR2).

[107] *In 1992, I arrived in the safety department, at this time it was called "inquiry office". The last 2 ou 3 years, we change our name we are now safety office.*

[108] *But there were also other reasons for not reporting. One is the fear to be fined, another is the "loss of face", because the old culture was that we don't make mistakes and yet another explanation is that reporting were not used in any proactive way at all. I think that we could have lived with the fine (or worse) if only the reports were also used for something else, so as to prevent the same thing from happening again. But the reports were only used to place blame. And another factor was definitely a very long and slow investigation process. We have several examples of cases, which have taken 2 years to investigate - only to find out that the controller was to blame and had to be fined. No other recommendations came out. This has also been a reason for not reporting. It is a very demanding task and very destructive to any human being to live in uncertainty for so long.*

Dans certains cas, l'erreur est encore vécue comme un tabou, y compris au sein des équipes de contrôle :

> *Non, personne ne confesse, j 'ai fait une faute, c'est une sorte de… c'est difficile à dire, oui, c'est difficile à dire : c'est moi qui ait fait une faute, c'est dur à dire. (un contrôleur Slovaque)*

En Suède, à l'inverse, le report d'incident est donc, globalement, très ancré dans les pratiques des contrôleurs. Il existe un consensus fort, entre la hiérarchie et les contrôleurs, sur le caractère normal, naturel, du report d'incident. Les raisons évoquées tiennent de l'éducation (*on nous enseigne cela dès notre formation initiale*), de la confiance, mais du sentiment, tout simplement, que c'est utile pour la sécurité, en termes de Retour d'expérience. A de nombreuses reprises, nos interlocuteurs ont insisté sur le caractère "non blamant" des investigations. Marlene Dyrløv Madsen et Thomas Ryan Jensen [109], qui ont comparé des analyses d'incidents danoises et suédoises, ont relevé le choix d'une grande neutralité dans le vocabulaire employé par les rapports suédois, qui ne portent pas de jugements de valeur sur les actions ou les décisions des contrôleurs, mais en décortiquent plutôt les mécanismes en termes cognitifs, et les replacent dans une vue systémique.

Une personne de l'autorité réglementaire explique l'origine de ce changement, qui remonte d'après son analyse aux années 50, par un changement chez les militaires. A cette époque, les militaires ont eu pendant quelques années de nombreux incidents et accidents. Ils ont choisi de lever les sanctions afin d'obtenir plus de données sur les incidents. Après avoir été blâmé et sanctionné, vivre et reporter un incident s'est transformé positivement au sein de l'organisation :

C'est même devenu bien de reporter si on était la seule personne à être au courant de l'incident qu'on avait vécu. Cela signifiait des valeurs d'intégrité, d'honnêteté, etc. *Lorsque le militaire et l'ATC civils ont fusionné, c'est la culture militaire qui a donné le ton. (Un responsable de l'autorité réglementaire).*

6.3.3. Un frein symbolique

Entre contrôleurs et pilotes, les relations sont ambivalentes, comme cela avait été souligné par le CETCOPRA[110]. Si les récriminations des pilotes (et d'ailleurs souvent, encore plus, des compagnies aériennes) vis-à-vis des contrôleurs sont bien connues (les fameux retards liés au contrôle du trafic aérien, qui font l'objet d'annonces parfois sarcastiques de la part des commandants de bord à leurs passagers), il n'en subsiste pas moins une forme de solidarité.

Or, pour un contrôleur, reporter un incident, c'est dans certains cas révéler une erreur ou une violation des procédures de l'équipage. Ce n'est pas du tout participer à un processus de Retour d'expérience, permettre de révéler un dysfonctionnement, mais plutôt "trahir" un collègue, "rapporter" comme on disait à la petite école… Un responsable sécurité raconte :

> *Vous connaissez Nice ? Ce sont des pilotes qui ont tourné à gauche en décollant face au Nord Est donc en plein vers la ville et la montagne par mauvais temps bien entendu. Donc le contrôleur en question disait : j'ai récupéré ça. Moi je n'ai pas laissé passer ça. J'ai appelé Nice et puis finalement il y a eu une petite enquête et je me suis rendu compte qu'il y a eu 3 cas comme ça, non connus, de gens qui ont tourné à gauche. C'est un cas où il aurait pu y avoir un accident, car là c'étaient des bimoteurs qui montaient assez vite mais avec un quadri ça ne passait pas la montagne. Or, on s'est rendu compte que c'était lié à un piège sur les cartes Jeppesen, à 300 pieds virage à droite tel cap, et sur une des standards (SID), une autre carte, cette carte présupposait que vous aviez la Jeppesen… et donc sur cette carte c'était "tournez à gauche" pour aller rejoindre telle balise et donc en fait là c'était des gens qui n'avaient pris que la carte SID où il n'était*

[109] Marlene Dyrløv Madsen & Thomas Ryan Jensen*: Fejl, ansvar og moral: Behandling af menneskelige fejl og udvikling af en professionsetik inden for flyveledelse og andre sikkerhedskritiske områder*. Technical Report R-1260, Risø National Laboratory, 4000 Roskilde Denmark. 2001.

[110] Gras, Alain, Moricot, Caroline, Poirot-Delpech, Sophie, Scardigli, Victor. *Face à l'automate : le pilote, le contrôleur, et l'ingénieur.* Publications de la Sorbonne, 1994.

pas rappelé qu'il fallait d'abord tourner à droite… donc un problème important restait caché, parce les contrôleurs ne voulaient pas dénoncer les pilotes, cette notion de dénonciation empêche… je dirais le report de tout ce qui n'est pas "perte de séparation"…

Donc si on prend cet exemple de Nice, ce n'est pas pour cacher des choses; c'est pour éviter des problèmes à des gens… bon de temps en temps il y a une responsabilité contrôle, c'est clair, mais le plus souvent, c'est une erreur type pilote et les contrôleurs ne veulent pas rapporter.

Cette solidarité autour d'un secret partagé ne peut manquer de faire penser au secret comme lien social évoqué par Simmel. Rappelons que Simmel propose une vision sociologique positive du secret : le secret n'est pas seulement la dissimulation, c'est aussi ce qui lie, ce qui rassemble.

Mais il n'y a pas toujours consensus au sein des contrôleurs, loin de là, sur ce secret à garder au sein d'une communauté pilotes/contrôleurs : entre le secret-valeur positive, et le secret-facteur de risque, certains pencheront pour la seconde compréhension. Mais comment parler d'un incident dans une organisation qui ne fournit pas obligatoirement les structures, les pratiques, d'un report qui ne serait pas vécu comme une forme de "dénonciation" ? Dans certains cas, il faut sortir de l'institution et, pour le coup, la publicité devient totale :

Il y a eu un incident très grave où une compagnie étrangère a descendu à 4 ou 5 nautiques de Lyon donc il a vraiment failli se planter dans les collines quand on se trouve face au nord, ça a été noté par le contrôleur, l'alarme[111] *a été identifiée, ça s'est passé le vendredi, et puis le mardi rien ne s'était passé, ou c'est resté coincé… ensuite vers le mercredi, il y a eu un article dans la presse locale, et vu le contenu, on soupçonne fort que ce soit un des contrôleurs sur place qui ne trouve pas normal que ce soit enterré ce truc-là, or c'est un événement très intéressant en termes de REX.* Un responsable sécurité français*.*

6.4. Le sens d'ASMT en fonction des organisations

Les éléments que l'on vient de voir dressent le tableau de pratiques, d'outils, de compréhension de la sécurité, de valeurs, de sens, différents dans chaque organisation. Bien évidemment, en fonction de chaque tableau, l'ajout d'un outil technique comme ASMT, prend une couleur différente. Dans nos entretiens, nous avons évoqué, soit l'installation prochaine d'ASMT (en Slovaquie, et en Italie, qui sont les deux pays ayant prévu son arrivée prochaine), soit l'existence de cet outil même si l'organisation n'est pas directement concernée.

, l'évocation d'ASMT auprès de contrôleurs (qui apprennent, à l'occasion de cet entretien, le projet d'installer ASMT dans leur centre !) suscite une méfiance non dissimulée, et des questions sur les procédures qui seront appliquées (qui aura l'information ? comment la confidentialité sera-t-elle protégée ? *etc.*). L'entretien prend alors une tournure émouvante :

Vous venez d'un pays démocratique… La France est depuis longtemps un pays démocratique, mais ici il y a encore des communistes, peut être la prochaine génération, il faudra demander à mon fils… OK (il rit)… je suis déjà un vieil homme, j'ai passé la moitié de ma vie sous le communisme, le contrôle tout le temps, c'était terrible, terrible… Un contrôleur.

Pour la hiérarchie du centre de Bratislava, l'enjeu est de taille. Dans quelques années, le nouveau Centre de contrôle aérien CEATS permettra de contrôler une partie de l'espace aérien supérieur du Centre et de l'Est de l'Europe. Le choix de la ville qui accueillera ce centre n'est pas encore effectué, et deux localités possibles sont Vienne et Bratislava. Il est clair que la mise en place d'un outil comme

[111] L'alarme MSAW (Minimum Safe altitude Warning)

ASMT est aussi une décision politique pour montrer qu'on est "transparent" sur les incidents, que l'on a rien à cacher en ce qui concerne la sécurité.

Le sociologue peut s'amuser à un peu d'ironie, puisqu'il n'y a pas d'incidents en Slovaquie *:*

> Question : *Mais que va vous apprendre ASMT ? si vous n'avez pas d'incidents ? si la sécurité est si bonne ? il ne va servir à rien ?*
> Réponse : *Qui sait ?… on aimerait qu'on nous fasse confiance, être les premiers de… de ce côté de l'Europe à avoir cet outil"*[112]*.* (Un responsable Sécurité).

on peut poser la question d'une façon un peu rhétorique : quel est le sens d'un "outil de la transparence" dans une organisation qui fait preuve d'une transparence certaine[113] ?*…* On pouvait faire l'hypothèse, que dans sa version "complément du report humain", il serait tout au plus jugé un peu inutile : si les incidents sont spontanément reportés dans leur grande majorité, à quoi sert-il de les détecter *automatiquement* ? L'outil soulève en fait des réactions qui vont bien au delà du doute. Il fait même, dans cette utilisation, l'objet d'un rejet très franc, de la part de la responsable opérationnelle du centre[114], elle-même ancienne contrôleuse :

> "*C'est l'opposé absolu de ce que nous sommes, je ne vois rien de bien avec cet outil, je ne crois pas que le système bénéficie de cela, cela voudrait dire que le management ne me fait pas confiance en tant que contrôleur*[115]*".*

Dans une organisation dans laquelle s'est construite une certaine transparence, associant confiance, culture non punitive, retour d'expérience, l'outil apparaît comme emblématique avant tout d'un manque de confiance de la hiérarchie (en tout cas de ceux qui auraient accès aux données ASMT) envers les contrôleurs, confiance qui semble être un des socles de ce qui s'est bâti à Malmö.

Ces trois exemples illustrent bien qu'un même outil prend une symbolique différente selon chaque place : cette symbolique va susciter des sentiments différents. Chaque organisation se construit un paradigme (Laroche) autour de la sécurité, qui intègre des aspects cognitifs, organisationnels, mais aussi symboliques, le tout étant étroitement intriqué. Mais on l'a vu avec l'exemple de l'installation d'ASMT à Maastricht, les choses ne sont jamais figées, tant qu'il reste une *marge d'indétermination* (Simondon) de l'outil qui permet de construire un usage satisfaisant pour tous les acteurs.

6.5. Quelle transparence vis-à-vis de l'extérieur ?

Dans ce chapitre on aborde la perception d'une organisation sur "sa" transparence, que ce soit vis-à-vis de l'autorité réglementaire, du grand public, *etc.* Il s'agit d'explorer l'auto appréciation que font les acteurs d'une organisation à risque, spontanément, quand on aborde cette question, qu'ils soient contrôleurs ou responsables de la sécurité. Ce qui nous intéresse ici, ce n'est pas tant le dosage (quoique certaines appréciations un peu véhémentes soient sans doute significatives d'un malaise de l'organisation…) que le sens que les personnes donnent à la transparence, à la possibilité ou à l'impossibilité de l'être.

---

[112] Who knows ? we would like to be trusted … to be the first in … in this side of Europe to get this tool.
[113] Dans ces entretiens, on a surtout abordé l'aspect symbolique d'ASMT. C'est le niveau qu'aborde spontanément la plupart des personnes interrogées. Les analystes d'incident s'intéressent aussi au côté "pratique" d'ASMT, qui permet une aide précieuse dans le dépouillement des données de l'incident.
[114] Nous n'avons hélas pas eu le temps d'aborder avec les contrôleurs leur perception de cet outil.
[115] *This is the absolute opposite of what we are. I don't see anything good with this, I don't think the system benefits of it … It would mean that the management does not trust me as a controller*

6.5.1. Avouer qu'un contrôleur prend des risques ?

Spontanément, lorsqu'on parle de transparence, un contrôleur italien évoque deux freins : la complexité et la prise de risque, cette dernière étant considérée comme "inavouable" : un extrait très parlant d'un dialogue avec deux contrôleurs à Rome :

> Question *: je travaille sur la transparence, qu'est-ce qu'on cache, qu'est-ce qu'on montre…*
> Réponse *: ce qu'on montre… très peu de choses car c'est difficile d'expliquer aux gens ce qu'est notre travail, et par exemple, la sécurité… comment peut-t-on expliquer. Tu travailles, et quelque chose peut bien se passer, ou se passer mal, si tu es assez sûr que quelque chose va bien se passer, tu acceptes la chose, mais tu n'es pas totalement sûr que cela va bien se passer, donc tu acceptes un risque, c'est un très très petit risque, mais tu l'acceptes, aussi comment peux tu expliquer à une personne qui va monter à bord d'un avion, à un passager*[116]*,…*
> *le second contrôleur ajoute : le passager pense qu'il n'y a aucun risque mais ce n'est pas vrai…*

Il est sûrement discutable que les passagers pensent qu'il n'y a aucun risque[117]. C'est bien connu, certains passagers ont peur en avion. Mais ce que ce contrôleur identifie de façon très intéressante, cependant, c'est que ce type de micro régulations, (tout n'est pas procéduralisé, prévu, et le contrôleur doit gérer une marge d'acceptation du risque) est très difficile à expliciter à un public. On en revient au problème sur l*e* "quantum d'information nécessaire pour la confiance" de Simmel : le public *doit* faire confiance pour des régulations qu'il ne peut appréhender, car elles exigeraient de lui une compréhension trop fine du travail du professionnel.

6.5.2. Etre Transparents sur quoi ?

La transparence des données incidents évolue.

> *Moi je pense qu'Eurocontrol a eu un impact important, jusqu'en 94-95, il n'y avait pas de gestion de la partie sécurité à Eurocontrol. Il y a eu la première réunion sécurité ça s'appelait le SMITF à l'époque : Safety Monitoring Improvement Task Force, c'était un embryon de ce qui est maintenant le S.I.S.G (Safety Improvement Sub Group) tu vois les pays n'avaient pas l'habitude de gérer, de parler sécurité entre eux, ni entre eux ni avec Eurocontrol et donc finalement dans l'ignorance de ce qui se faisait, de ce qui se tramait chez les voisins on cachait.*
> *Puis ce S.I.S.G, enfin le SMITF a été crée, on était 3 pays au début, l'Angleterre, l'anglais était déjà là, nous les français, et le 3ème je crois que c'est le Suédois, après il y a eu un Hollandais, ça a été long à se mettre en place. (…) Quand tu vois le voisin faire, comme il me donne ses chiffres et pas seulement ses chiffres, sa méthode de calcul, d'analyse, les grandes causes le bilan, chacun s'est fait devant les voisins son bilan sécurité et bien tacitement en fait tout en rebouclant en interne, je pense, en tout cas, c'est ce que j'ai fait chez moi, qu'est-ce qu'on donne, qu'est-ce qu'on livre, est-ce qu'on censure ou non, personnellement je ne voulais pas donc j'ai dit, ce serait bien qu'on puisse tout dire et tout et à l'époque mon chef direct a convenu qu'il fallait tout dire. Dès ce moment là, il m'avait demandé, comment ça se passait quand même, on s'est dit, bon on joue la transparence c'était nouveau tu sais à l'époque la transparence. On est transparent… (…)*

---

[116] *Very little is shown because it is difficult to explain to people what our work is, what is our job, and for instance safety, how you can explain … you work and something can go wrong, or something can go ok, so if you are quite sure that something goes ok, you accept the thing, but you are not sure it is ok, so you accept the risk, it is a very very little risk, but you accept it, so how can you explain this to a person going aboard an airplane , to the passenger*

[117] Christine Noiville fait remarquer que "le public cherche moins le risque zero que le "mépris zéro" : information et confiance jouent ainsi un rôle essentiel dans la formation du jugement individuel sur le risque". *Le Risque acceptable, une vision juridique*. Colloque CNRS Risques collectifs et situations de crise. Février 2000.

enfin, Il y a 800 TCAS on ne s'affole pas de le dire. On n'est un peu moins transparent déjà, et même beaucoup moins transparents sur les causes.

6.5.3. Des limites

La transparence a des limites… que certains épinglent avec une certaine véhémence :

Est-ce que nos organisations sont suffisamment transparentes du point de vue de la sécurité ? NON, on ne va pas tourner autour du pot, c est non. Est-ce que la sécurité est vraiment l'enjeu primordial ? c'est un enjeu majeur… vous voyez toujours le même discours… (Un responsable sécurité français)

Et que d'autres tempèrent :

La transparence je dirais… elle a ses limites déjà, et c'est un concept qu'on affiche quand on est capable de maîtriser la gestion de la sécurité. C'est à dire on sait ce qu'on va trouver, parce qu'on sait quels outils on a, on sait ce qu'on est capable d'en faire et on se donne une limite, cela, c'est personnel ce que je te dis, dans la diffusion de l'information obtenue. La transparence totale je n'y crois pas vraiment et qu'est-ce qu'on entend par transparence ? Est-ce que c'est être transparent sur les chiffres, sur les faits, sur l'analyse, sur les conséquences ? En France depuis 2 ou 3 ans on dit "on est transparent". (Un responsable sécurité français)

Un exemple :

Ce que j'ai tendance à dire depuis 2 ans même si ça va s'améliorer, le doublet à Charles de Gaulle par exemple, le fonctionnement en doublet est dangereux. C'est à dire de poser et de décoller comme ça en parallèle sur 2 pistes très proches, c'est dangereux parce qu'actuellement les méthodes ne sont pas clairement établies. Tu ne peux pas le dire ça, la transparence a ses limites, parce qu'on va dire mais Machin, attendez si vous dites ça mais on arrête Charles de Gaulle et puis qu'est-ce qu'on devient, ce n'est pas pensable, on va nous répondre mais le doublet a été mis en place, regardez maintenant on est passé à tant de milliers de vols par jour 1500 vols par jour, tout le monde est content, on a réduit les retards, les passagers sont contents, économiquement c'est bénéfique alors vous avec vos 3 Airprox, vos 10 incidents, tu vois ce n'est pas grand chose. Tu vois, la transparence a quand même ses limites… (Un responsable sécurité français)

6.5.4. L'évaluation du risque

La Safety Regulation Unit a demandé le report des incidents mais aussi une évaluation du risque pour chaque Airprox, afin de procéder à des classifications. Le risque est classée en 5 classes, de A à E, le risque A correspondant au risque le plus grave (risque d'abordage). Le document ESARR 2 donne des indications précises pour aider le classement. Elle s'est inspirée des pratiques françaises. Par exemple, un incident au-dessous de la demi-norme mène en général à une classification en risque A (sauf, par exemple, s'il y a eu séparation à vue). De même, un TCAS RA (Avis de résolution) justifié mènera aussi en général à une classification en A[118]. Mais tout n'est pas si simple, un responsable français explique :

Tu prends le même incident analysé par l'Angleterre, la France et l'Italie tu n'auras pas le même risque. J'ai discuté avec des anglais, je leur ai dit : comment ça se fait que sur 180 Airprox par an, vous en avez 80% où vous dites "risque nul", alors que nous on n'a que 20% de risque nul ?! C'est vite vu, à partir du moment où il y a un R.A TCAS, ça passe

[118] Le TCAS s'appuie sur des données temporelles : il déclenche 25 secondes avant un abordage possible des deux aéronefs. Dans la majorité des cas, cela correspond aussi à une distance de séparation inférieure à la demi-norme.

près un RA TCAS… nous, on met au minimum A ou B, risque fort, et eux, pour raccourcir, complètement l'inverse. Les anglais disent : le RA TCAS a déclenché, donc il n'y a pas de risque… et c'est là qu'Eurocontrol mélange des navets et des carottes !

Le groupe SISG a été l'occasion de confronter des pratiques différentes selon les pays. La catégorisation française, et la classification SRC qui s'en est inspirée, si elle prend d'autres critères que la distance de séparation entre aéronefs, conduit de facto à une catégorisation d'une majorité des AIRPROX en A ou B, tandis que la classification du NATS (qui propose une fiche d'évaluation du risque qui attribue des points en fonction de nombreux critères) classe plus d'AIRPROX en C. Le NATS a présenté son système de classification, et discuté avec d'autres pays (notamment l'Italie, et l'Allemagne) qui ont été convaincus de la pertinence de cette méthode d'évaluation du risque. Mais *quid* alors de la conformité à ESARR 2 ?

En Italie, on discute :

J'ai parlé à P. Stasny[119], je lui ai dit que je n'étais pas d'accord pour appliquer ESARR 2 de cette manière, je suis conscient que ESARR 2 est très officiel, mais peut être nous pouvons dire quelque chose, pas effacer, intégrer. Je lui ai dit : "quand vous dites : si la séparation est inférieure à tant de miles ou pieds", il faut classer en "A", c'est un exemple, seulement un exemple ?"

Une fois convaincus par la méthode du NATS, il faut convaincre les analystes d'incidents, de tempérer leur évaluation du risque, qui semblait assez proche, jusqu'à présent, de la façon de faire française. Il faut "changer leur cerveau" !

Avec cette nouvelle procédure, les analystes doivent modifier leur point de vue, penser avec un autre esprit, un autre cerveau… il est important de dire aux analystes : si le TCAS a déclenché, ce n'est pas nécessaire de penser tout de suite : "c'est un très gros AIRPROX". Vous devez tempérer avec tous les indices du système d'évaluation, vous devez équilibrer[120]. (un responsable sécurité italien).

A la direction de la Navigation Aérienne française, très récemment, on s'est inquiété des chiffres français pour l'année 2000, comparés à d'autres pays : ils font apparaître, comme l'avait pressenti le responsable sécurité que nous avions interrogé voici environ un an, que les AIRPROX français sont très sérieux (beaucoup de risques "A"), alors que beaucoup d'autres pays ont des AIRPROX sans gravité (C et en-dessous)… C'est effectivement ce qu'une lecture rapide des statistiques fournies à la SRC laisse penser[121].

Ce qu'on peut retenir de ces débats, c'est combien l'évaluation du risque se construit au sein de l'organisation, combien elle dépend de paradigmes de compréhension de la sécurité différents. Ces paradigmes ne sont pas étrangers à une contrainte de publicisation de l'information. Une partie des pays finit par adopter la méthode d'évaluation du risque proposée par le NATS, qui, certes, propose une solide base de réflexion sur ce qu'est le risque, mais qui aboutit, accessoirement (?), à catégoriser peu d'AIRPROX dans la catégorie A, risque maximum. La Direction de la Navigation Aérienne française a décidé de mener une enquête sérieuse sur les méthodes effectivement adoptées par les pays d'Europe, plus ou moins séduits semble-t-il par la méthode du NATS, et par conséquent plus ou moins proches des consignes données par ESARR2… En attendant, la DNA a décidé de restreindre pour la première fois cette année la diffusion de son Bilan sécurité 2000 (qui décrit les AIRPROX et HNRN français, ainsi que les défaillances identifiées) : ce bilan ne sera pas distribué aux compagnies

[119] Monsieur P Stastny est le chef de la SRU.

[120] *Until 4 months ago, investigators, if you were evaluating an AIRPROX taking into account a lot of topics, but at the end the vertical distance creates something mandatory … with this new procedure, investigators have to modify their old point of view, and to think with another mind, with another brain, it is important before to issue this to say to investigators, from now you have to think that if the TCAS RA is blinking, it is not necessary to interpret it as something as "this is a very big AIRPROX, you have to mitigate with the whole cues of the scoring system, that you have to evaluate, you have to balance.*

[121] Gardons nous de tout chauvinisme : il se peut, que même en harmonisant les évaluations du risque, les français conservent une petite avance sur les AIRPROX sérieux, mais il est indubitable à première vue que les différents mécanismes d'évaluation jouent un rôle primordial.

aériennes et au SISG. La transparence, oui, mais si tout le monde joue le même jeu : c'est aussi à cela que sert l'harmonisation…

6.6. L'analyse et le feed back

6.6.1. Les insuffisances actuelles

Cet aspect a été peu abordé puisqu'à travers les questions sur la transparence, c'est sur le processus qui se situe en amont de l'analyse que l'attention a été portée. Evidemment, tout est très lié : on a identifié les divers éléments (cognitifs, organisationnels) qui définissaient le paradigme qui sous-tend la collecte de données, et comment ce paradigme se renforçait avec les outils techniques qui se développent. Avec la notion d'*énaction* de Weick, on a montré que dans la transparence, on ne dévoile pas une "vérité" préexistante, mais que l'on crée des catégories de l'information recherchée, notamment en fonction de la norme.

L'analyse des incidents est peu ou pas outillée en termes méthodologiques ou conceptuels. Les analystes font de leur mieux, et malgré l'aide de techniciens qui les secondent, une partie importante du temps est consacrée aux tâches laborieuses de retranscriptions de la fréquence, *etc.* Parmi les organisations rencontrées, les Suédois sont sans doute les plus portés à proposer des analyses fines, en s'attachant à une vision systémique.

Une étude récente de Cyril Barriquault, réalisée dans différents CRNA et approches françaises, a montré que de nombreux biais dans le processus d'analyse et de codage des causes des incidents. Par exemple, l'analyse s'arrête après la découverte d'une cause typique et fréquente. En outre, "*les enquêteurs privilégient dans leur compte-rendu les éléments pour lesquels ils pensent à une solution associée, et inversement, ils suppriment de leur compte-rendu les éléments pour lesquels ils imaginent moins facilement une solution (un changement profond d'organisation du travail, de hiérarchie ou de matériel).* Par conséquent, les problèmes organisationnels ou politiques sont peu évoqués (et ce, encore moins dans les fiches écrites qu'à l'oral, lors des discussions qui précèdent la rédaction).

Un exemple nous montre bien cette différence entre ce qui est compris, et ce qui est finalement écrit dans le rapport :

> *Dans les incidents récents on a par exemple appris, quand je dis on c'est la DNA, parce on a rappelé la QS. Le dossier n'était pas très clair, on leur a dit : pourquoi le contrôleur était-il encore là ? il mentionne la fatigue, il attendait la relève, qui ne vient pas, et ils nous ont expliqué, et cela c'est une défaillance organisationnelle, c'est qu'ils ne pouvaient pas être relevés car ceux qui devaient relever attendaient eux mêmes une relève de gens qui n'étaient pas arrivés… le système prévoyait une relève par des gens déjà en poste… personne ne se relevait, c'est un cas extrême, mais d'après ce qu'ils m'ont dit, c'est très fréquent, parfois les contrôleurs ne sont pas arrivés, et cela ce n'est pas écrit dans les analyses, ils n'osent pas écrire des choses comme cela… (un responsable sécurité français)*

L'étape suivante, le "feed back" hérite bien sûr des insuffisances de l'analyse. Dans divers discours se focalisant sur la collecte sans faille des incidents, on peut retrouver cette notion de transparence vécue comme fin en soi, dont on oublie la visée ultime. Il s'agit bien sûr aussi d'une question de maturité. L'idée sous jacente est de sérier les problèmes : on a pour le moment peu d'informations sur la sécurité. "*Organisons la collecte, la classification et on verra ensuite ce qu'on en fait*", semble être un mot d'ordre plus ou moins explicite. A noter aussi qu'il y a toujours en arrière plan, l'idée d'être "à la traîne" par rapport aux compagnies aériennes, qui ont, pour la plupart organisé et réglementé le REX depuis plus longtemps. Dans ce contexte, le monde de la navigation aérienne se perçoit souvent comme le mauvais élève.

6.6.2. Les régulations locales du risque

L'exemple Suédois (plus précisément, l'exemple de Malmö) montre l'intérêt d'un traitement local des incidents, avec ce que Cyril Barriquault appelle une *boucle courte* de Retour d'Expérience. Les "*événements dont on peut apprendre*" sont discutés localement, ils gardent toute leur richesse grâce à la connaissance du contexte qui est ainsi maintenue, alors que le codage dans une base de donnée mène toujours peu ou prou à un appauvrissement de l'information retenue. Après le "*traitement local*" vient le "*remède local*". Le "remède local" ne consiste pas en une prise de décisions fracassantes qui n'ont pas leur place ici : comme le rappelle la recherche effectuée par Cyril Barriquault : "*les incidents mineurs et encore plus leur contrôle, font partie de la régulation du travail normal; ils reflètent l'expertise des acteurs de première ligne qui gèrent les adaptations du système homme machine au contexte*". Il s'agit donc de permettre aux contrôleurs de travailler sur une "auto-transparence" locale, qui permet *in fine* un meilleur réglage de la prise de risque, de l'efficacité des micro-régulations effectuées par les équipes. Les évènements rapportés peuvent permettre d'identifier, par exemple, qu'une petite violation routinière que tout le monde fait, peut dans une configuration précise, être dangereuse, qu'un raisonnement "*par défaut*" qui est valable dans la majorité des cas est faux avec telle performance d'avion, *etc.*

Cette solution suédoise donne de nombreuses pistes de réflexions pour les questions qui ont été abordées jusqu'à présent. Avec l'exemple du trading, nous avions vu comment une pratique de "reporting" journalier du trader incitait chaque professionnel à expliciter ses raisonnements "*parce que ça te pousse aussi à plus réfléchir sur quelles pos tu prends, pourquoi*", et comment cet effort pour être "*plus transparent à soi-même*" était vécu comme une dimension de la régulation du risque. Là où le dialogue se fait entre chaque trader[122] et son chef de "desk", la régulation dans l'exemple suédois est collective, mais il existe bien sûr une parenté. Toutefois, cette régulation fine du risque n'est pas plus "*publicisable*" chez les contrôleurs qu'elle ne l'est chez les traders. Comme l'exprimaient nos contrôleurs italiens : "*tu acceptes un risque, c'est un très très petit risque, mais tu l'acceptes, aussi comment peux-tu expliquer à une personne qui va monter à bord d'un avion, à un passager*". Au fantasme d'une organisation totalement transparente sur tous les évènements, s'opposerait l'idée d'une *transparence suffisante* qui saurait laisser le traitement de certains événements à un échelon local. Ce qui est d'ailleurs à l'œuvre dans d'autres industries à risques : le directeur sécurité d'Elf Atochem explique "*nous avons décidé que l'analyse se ferait au plus proche de l'événement. (…). Pour autant qu'ils aient la compétence, les moyens et la disponibilité, ce sont forcément les gens qui ont vécu cet événement qui sont à même d'effectuer la meilleure analyse et d'en tirer le plus grand profit. De plus, je tiens à ce qu'on les laisse dans leur intimité*"[123].

Ce qui n'exclue pas une remontée d'informations synthétiques par l'encadrement local au chef de site chez Elf Atochem. Dans le cas précis de la Suède, ce traitement local est complété par le consultant qui fait un travail de synthèse (il défend l'importance d'un regard extérieur pour un bouclage vers l'identification de *patterns*). Etant donné la mise en place très récente (6 mois) du traitement local des incidents, on ne dispose pas de résultats sur cet aspect.

Il semble que les organisations qui ont développé ces procédures de traitement local d'incidents par des acteurs de première ligne sont aussi celles qui avaient déjà une organisation très solide de Retour d'Expérience plus classique, avec analyse centralisée des événements, *etc.* Il faudrait explorer d'autres exemples pour identifier s'il y aurait là quelque chose de l'ordre d'un processus de maturité dans le retour d'expérience.

---

[122] Ce qui est vrai pour l'analyse des actions a posteriori. On a vu qu'il existait aussi une régulation collective, orchestrée par le chef du Desk, en Temps Réel. Voir Chapitre 3.

[123] Yvan Verot. *Maîtrise du risque dans l'industrie chimique et pétrochimique : retour d'expérience*. Séminaire CNRS. Mars 1998

6.6.3. les régulations organisationnelles des risques : la mise sur agenda

Cependant, des actions organisationnelles sont également nécessaires. Des défaillances du fonctionnement du système relèvent aussi d'actions à prendre par la hiérarchie, ou par des instances internationales (autorités réglementaires par exemple). Pour prendre des exemples concrets, les contrôleurs ne peuvent traiter à leur niveau la modification d'une procédure que l'on finit par juger dangereuse, les lacunes dans la formation, le reclassement d'un espace aérien, la relation avec les compagnies aériennes pour réfléchir à l'impact du TCAS sur la relation entre pilotes et contrôleurs, *etc.* Ce que les sociologues appellent depuis peu la "mise sur agenda" des risques, c'est-à-dire, la prise de conscience d'un risque par un collectif, et son ancrage dans des processus décisionnaires implique toute l'organisation des acteurs de première ligne à la direction, et même, c'est ce que nous tenterons de montrer tout de suite *l'inter-organisationnel.*

Si on prend succinctement l'exemple de la mise sur agenda du problème des "incursions de piste" dans la communauté de l'aviation civile, on peut articuler les notions de *secret structurel* (pour rappel, Diane Vaughan avait utilisé la notion de secret structurel pour montrer comment des aspects structurels et fonctionnels dans l'organisation toute entière avaient permis l'*affaiblissement* des signaux d'alarme quant aux limites de résistance des joints de la navette), de *décision stratégique* (Hervé Laroche s'interroge sur l'accession des problèmes à l'attention des dirigeants, et montre comment le paradigme dominant peut empêcher la prise de conscience d'un problème) et de *Sensemaking* (de Weick). Ecoutons un responsable sécurité français :

> *Les américains ont les initiatives "safer sky", ils identifient les items les plus importants. Les JAA aussi. Jusqu'à il y a un an, les runway incursions, ce n'est pas un problème pour eux. On les a embêtés là dessus, il y avait une conscience qu'il y en avait mais ils ne sont pas connus. Maintenant que le responsable du JAA a les chiffres de Roissy (nombre de RI par décollage), ils ont été ahuris parce que pour eux dans l'optique SFACT des chiffres comme cela pour un élément critique serait inadmissible. A Roissy c'est le seul endroit en Europe où on ait les chiffres, grâce aux ASR et au reporting de contrôleurs, on en a quelques uns, on a de beaux graphiques avec l'évolution des RI qui maintenant circulent partout quitte à ce qu'on se fasse passer pour des mauvais élèves mais il n' y a pas de raisons ça doit être partout pareil. Donc maintenant les JAA ont décidé de lancer une activité dans ce domaine, clairement les gens n'avaient pas conscience du problème sur ce thème-là. Maintenant qu'on en a conscience, on commence à connaître aussi des incursions de pistes en dehors de Roissy, on a du en avoir 5 ou 6 on passe de zero a 5 ou 6 rapidement !*

A noter qu'il existe maintenant depuis peu une "Runway safety initiative" d'Eurocontrol.
Cette notion de mise sur agenda repose les problématiques de la transparence, en les couplant avec les processus de décision. En fait, on a vu combien il serait artificiel de séparer les processus de mise en transparence (qu'est-ce que j'obtiens comme informations sur mes risques, mes défaillances) et de décision (une fois que j'ai collecté, qu'est-ce que je fais ?). Avec la notion de "sensemaking" on a montré que la construction de sens était un processus créatif d'énaction des informations. La focalisation sur un type d'informations (les pertes de séparations en vol) va mettre dans l'ombre d'autres problèmes (les incursions de pistes). La collecte d'informations se heurte à des limites juridiques, structurelles, symboliques comme on l'a vu plus haut. L'interprétation, qui est une partie du sensemaking, va se heurter à des limitations cognitives (biais) comme l'a montré l'étude de Barriquault déjà citée, et organisationnelles (*les analystes d'incidents n'osent pas écrire…*). Quant aux problèmes de l'appauvrissement des informations lors du codage dans les bases de données, il demande une réflexion sur la formation nécessaire pour les analystes, sur la limite de la classification des incidents. En outre, Cyril Barriquault remarque (communication personnelle) que les analystes d'incidents ont souvent développé, sur la base de leur expérience, une intuition très fine, par nature difficilement formalisable, de l'incident *vraiment intéressant* qui révèle un aspect laissé dans l'ombre des défaillances du système. Il faudrait désormais réfléchir dans une perspective de "formulation des problèmes stratégiques" comme le propose Hervé Laroche, en prenant en compte tous les niveaux de l'organisation.

Chapitre 7.Conclusion

Ce que je vous raconte, vous n'allez pas le donner à la Presse, au moins ?

Un responsable sécurité

Ce travail a permis d'explorer les trois angles de la notion de transparence, et de les mettre à l'épreuve d'un problème concret (la visibilité des incidents, la perception des risques) dans le contrôle de la navigation aérienne.

Cette notion a été abordée d'abord sous l'angle de l'*auto-transparence* et en cela elle est emblématique de la modernité. Lorsqu'il s'incarne dans une organisati

montré les travers et le coût sociologique dans le domaine du nucléaire. La transparence comme une forme de régulation du risque nous paraît aussi une notion à creuser dans un futur travail, ainsi que le lien que le professionnel *en première ligne* fait entre *sa* transparence et le sens donné à cette valeur dans l'organisation, (qui d'autre est transparent, et qu'en fait-on ?) dans le prolongement de ce qui a été exposé dans l'exemple du trading.

Dernier angle de notre exploration, *la transparence de l'organisation* ne peut se passer de la notion de confiance. On a montré qu'un projet de "*transparence totale*" n'était au mieux qu'une formule en forme de slogan employé par un acteur politique souhaitant afficher (sincèrement, pourquoi pas, nous lui en faisons volontiers crédit) un tournant dans la gestion de la sécurité d'une grande industrie en perte de… confiance justement. Or, toute organisation comporte sa part de *négociations implicites* qu'il est inutile de vouloir formaliser. Cependant, et c'est là tout le dilemme, comme d'autres organisations de ce type, le contrôle de trafic aérien se devra sans doute d'être de plus en plus garant de cette "*constance institutionnelle*" (La Porte) qui permet de garder la confiance du public sur la durée, donc redevable d'une forme de transparence dont il reste à déterminer le contenu, en gardant à l'esprit l'élégante formule de Simmel : *La confiance est aussi un état intermédiaire entre le savoir et le non savoir. Celui qui sait tout n'a pas besoin de faire confiance, celui qui ne sait rien ne peut raisonnablement même pas faire confiance*. La phrase de Christine Noiville, rappelant que le public ne désirait pas tant le *zéro risque* que le *zéro mépris* nous paraît à cet égard emblématique des enjeux actuels. Certes la transparence est aussi un instrument de communication, parfois un slogan, mais elle n'est pas que cela. J'en veux pour preuve les entretiens toujours nourris et souvent passionnés qu'à provoqué ce thème de recherche dans les entretiens qui ont accompagné ce travail.

Bibliographie

Amalberti, René. *Approches ergonomiques des erreurs et du risque.* Colloque CNRS Risques collectifs et situations de crise. Février 2000

Amalberti, René et Barriquault, Cyril. *Fondements et limites du Retour d'Expérience*. Annales des ponts. Septembre 1999.

Barriquault, C. & Amalberti, R. L'influence des modèles de causalité sur l'analyse d'incident de contrôle aérien. Congrès SELF, Caen. 1999.

Arendt, Hannah. *Condition de l'homme moderne.* AGORA, Calmann Levy. 1983.

Belorgey, Jean-Michel. *L'état entre Transparence et Secret.* POUVOIRS. N°97. Avril 2001.

Birraux, Claude. Le contrôle de la sûreté et de la sécurité des installations nucléaires. Economia. 1992.

Blaize, Martine. Safety regulation commission SRC Doc 2. "Aircraft Accidents/incidents and ATM contribution".

Bourrier, Mathilde. Le Nucléaire à l'épreuve de l'organisation. PUF. 1999.

Bredin, Jean Denis. *Secret, Transparence et démocratie.* POUVOIRS, N°97. Avril 2001.

Breton, Philippe. Le culte de l'Internet : une menace pour le lien social ? La Découverte. 2000.
Bulletin de la sécurité aérienne. DNA. Décembre 2000.

Carcassonne, G. *Le trouble de la transparence.* POUVOIRS, n°97. Seuil. Avril 2001.

Carlberg, Ingrid. *L'opaque Transparence de l'Union Européenne.* Le Monde Diplomatique. Juin 1997.

Chevallier, J. Le mythe de la transparence administrative. CURRAP, n° 679. 1988.

Crozier Michel et Friedberg Erhard. L'acteur et le système. Points, Seuil, 1979.

De La Burgade, Denis. *La vie privée des hommes politiques.* Thèse de doctorat, Paris I. 2000.

Madsen Marlene Dyrløv & Ryan Jensen Thomas*: Fejl, ansvar og moral: Behandling af menneskelige fejl og udvikling af en professionsetik inden for flyveledelse og andre sikkerhedskritiske områder*. Technical Report R-1260, Risø National Laboratory, 4000 Roskilde Denmark. 2001. (présenté en anglais par les auteurs).

EATMP Guidance Material "Reporting Systems" SAF.ET1.ST01.1000-GUI-01-00,Human Reporting.

ESARR 2 : "Notification et analyse des évènements liés à la sécurité dans le domaine de l'ATM".

ESARR 3 : "Use of Safety Management Systems by ATM service providers"

Eurocontrol Safety letter, EATMP Safety Group.

Fenwick, Lindsay. Access to data : Privacy, Proprietary and Unions Issues. International Symposium on Transportation Recorders. Arlington. 1999.

Foucault, Michel. *Surveiller et punir*. Tel, Gallimard. 1975.

Friedberg, Erhard. *Le pouvoir et la règle.* Seuil. 1993.

Friedberg, Erhard. Communication orale. "*La maîtrise des risques majeurs par la connaissance approfondie des organisations*". Table ronde du 15 novembre 2000 organisé par la société NORM.

Gérard, P. Ost, F. Van de Kerchove, M. *Actualité de la pensée juridique de Jeremy Bentham.* Facultés universitaires de Saint Louis. 1987.

Gras, Alain. *Grandeur et dépendance.* PUF. 1993.

Gras, Alain, Moricot, Caroline, Poirot-Delpech, Sophie, Scardigli, Victor. *Face à l'automate : le pilote, le contrôleur, et l'ingénieur.* Publications de la Sorbonne, 1994.

Gras, Alain. *Anthropologie et sécurité*, Colloque sur les risques. CNRS. Gif-sur-Yvette. 1999.

Holton (Captain Mike Holton). *FOQA : Aviation's most important safety tool.* British Airways. 52 FSF Annual International Air Safety Seminar, 29th IFA international conference and IATA. November 1999.

Hustvedt, Siri. *Yonder.* Henri Holt. 1998.

Hans Jonas, le principe Responsabilité. Champs Flammarion. 1995.

K., Joseph (haut fonctionnaire). *Opacité à la française, cet archaïque secret d'Etat.* Le Monde Diplomatique. Juillet 2000.

Kaufmann, J-P. Voyeurisme ou Mutation Anthropologique ? Le Monde. 10/05/01.

Kessler, Denis. *L'entreprise entre Transparence et Secret.* POUVOIRS, n°97. Seuil. Avril 2001

La Porte, Todd. Colloque Risques. Gif sur Yvette. Mai 2001.

Laroche, Hervé. *Risque, Crise et problématique de la décision dans les organisations*. Séminaire Risques collectifs et situations de crises. 15 Novembre 1995.

Lassalle, J.P. *La Démocratie américaine.* Colin, 1991.

Laval, Christian. *Jeremy Bentham*, *Le pouvoir des fictions.* PUF, 1994.

Lenoir, Noëlle. *Conclusion.* Actes du colloque organisé par le CEDORE (Nice) sur "La transparence dans l'Union européenne. Mythe ou principe juridique ?" L.G.D.J. 1999.

Lequesne, Christian. *La Transparence, vice ou vertu des démocraties.* Actes du colloque organisé par le CEDORE (Nice) sur "La transparence dans l'Union européenne. Mythe ou principe juridique ?" L.G.D.J. 1999.

Lequesne. *L'état entre Transparence et Secret.* POUVOIRS. N°97. Avril 2001.

Machiavel, Nicolas. *Le Prince*. Traduction de Jacqueline Risset. Babel, Actes Sud. 2001.

Moricot, Caroline. *Des avions et des hommes.* Septentrion. 1997.

Noiville, Christine. *Le Risque acceptable, une vision juridique.* Colloque CNRS Risques collectifs et situations de crise. Février 2000.

Perrow, Charles. Organisations à risques et "normal accidents". Point de vue de C. Perrow. Séminaire Risques collectifs et situations de crises. Quatorzième séance, 2 juin 1999.

Poirot-Delpech, Sophie. Biographie du CAUTRA. Thèse de Doctorat, Paris I.

Poirot-Delpech, Bertrand. *Fausses Transparences.* Le Monde. 17/04/01.

Rideau, Joël. *Jeux d'ombre et de lumière en Europe.* Actes du colloque organisé par le CEDORE (Nice) sur "La transparence dans l'Union européenne. Mythe ou principe juridique ?" L.G.D.J. 1999.

Sagan, Scott. D. *The limits of Safety.* Princeton University Press. 1993.

Saul, Jessie E. The Transparency of Blood, The construction of risk and safety during and after the AIDS blood scandal in France and the US. Workshop on Social Construction of Risk and Safety, Villa Fridhem, Kolmården, Sweden. March 15-17, 2000.

Secret et lien social. Actes du colloque Secret et société, Université de Lausanne. L'Harmattan. 2000.

Simmel, G. *Secret et sociétés secrètes.* Circé. Poche. 2000. (Première édition : 1908).

Simondon, Gilbert. *Du mode d'existence des objets techniques.* Aubier, Philosophie. 2001.

Torres, Anne. Interview, Le Prince de Machiavel - Théâtre des Amandiers, Nanterre. Le magazine Littéraire, N°397. Avril 2001.

Trigano, Shmuel. *La transparence opaque. La Shoah entre "abus de mémoire" et "idéologie moderne".* POUVOIRS, n°97. avril 2001, Seuil.

Vattimo, Gianni. *The Transparent Society.* The John Hopkins University Press, Baltimore. 1992.

Vaughan, Diane. *The Challenger Launch Decision.* Chicago Press. 1996.

Verot, Yvan. Maîtrise du risque dans l'industrie chimique et pétrochimique : retour d'expérience. Séminaire CNRS. Mars 1998.

Wallace, H. *Transparency and the legislative process of European Union.* Actes du colloque organisé par le CEDORE (Nice) sur "La transparence dans l'Union européenne. Mythe ou principe juridique ?" L.G.D.J. 1999.

Weick, Karl. *Sensemaking in organisations.* Sage Publications. 1995.

Westrum, Ron. (1991). *Technologies & society: The shaping of people and things*. Belmont, CA: Wadsworth Publishing Compan.