UCLouvain

Faculté des sciences économiques,
sociales, politiques et de communication

Les stratégies de communication adoptées par les entreprises lors de crises liées à des fuites de données, avec un focus spécifique sur les perceptions des parties prenantes et les meilleures pratiques observées

Quelles stratégies de communication une entreprise met-elle en place auprès du grand public en cas de fuite de données ?

Auteur : Neu Guillaume
Promoteur : Scieur Philippe
Année académique 2025-2026
Master 120 en communication, à finalité communication stratégique des organisations (Louvain-la-Neuve)

RÉSUMÉ

Ce mémoire interroge les stratégies de communication déployées par les organisations lorsqu'elles font face à une fuite de données. Il s'agit d'une crise organisationnelle spécifique, à la fois technique et symbolique, qui expose simultanément la sécurité informatique et la réputation de l'organisation. La question de recherche centrale est la suivante : quelle stratégie de communication une entreprise met-elle en place auprès du grand public en cas de fuite de données ?

Le cadre théorique mobilise la communication corporate, la communication de crise et deux théories de référence, la Situational Crisis Communication Theory de Coombs et l'Image Repair Theory de Benoit, qu'il croise avec la littérature spécifique aux fuites de données et à la protection des données personnelles. Cette synthèse débouche sur un modèle d'analyse à cinq dimensions — temporalité, stratégie discursive, canal de communication, public visé et registre du message, action corrective — et sur quatre hypothèses de travail portant respectivement sur la rapidité et la transparence, l'adéquation entre stratégie discursive et niveau de responsabilité, l'usage dialogique des réseaux sociaux, et le rôle de l'action corrective dans la reconstruction de la confiance.

La partie empirique met ce modèle à l'épreuve du terrain à travers une démarche qualitative en deux volets : cinq entretiens semi-directifs conduits auprès de professionnels de la communication, de la sécurité informatique et de la gestion de crise, ainsi que l'analyse de quatre cas réels de communication post-incident, situés principalement en Belgique et au Luxembourg dans des secteurs financier et régulé. Les résultats confirment globalement les prescriptions théoriques, tout en révélant un apport original non anticipé par le cadre initial : le paradoxe de l'aveu de négligence, selon lequel une action corrective peut renforcer ou au contraire éroder la confiance selon qu'elle est perçue comme une preuve de maîtrise ou comme l'aveu tardif d'une faille déjà connue. Le mémoire se conclut par des recommandations pratiques à destination des organisations, portant notamment sur la préparation en amont de la crise, la coordination entre cellule technique et cellule de communication, et la nécessité d'anticiper les questions implicites que soulève toute action corrective.

MOTS-CLÉS

Communication de crise · Fuite de données · Réputation organisationnelle · Confiance · Situational Crisis Communication Theory · Action corrective

REMERCIEMENTS

Je tiens tout d'abord à exprimer ma profonde gratitude à mon promoteur, Monsieur Philippe Scieur, pour sa disponibilité, ses encouragements et la pertinence de ses conseils tout au long de la réalisation de ce mémoire.

J'adresse également mes sincères remerciements à l'ensemble des professeurs du Master en communication pour la qualité de leur enseignement, qui a largement contribué à ma réflexion, ainsi qu'au secrétariat du département de communication pour son professionnalisme, sa disponibilité et sa bienveillance.

Mes remerciements s'adressent tout particulièrement aux professionnels et aux experts qui ont accepté de me consacrer du temps dans le cadre des entretiens. Le partage de leur expérience, de leur expertise et de leur vision du terrain a constitué une contribution essentielle à ce mémoire.

Je remercie chaleureusement toutes les personnes qui ont contribué, de près ou de loin, à l'élaboration de ce travail. Leurs remarques, leurs suggestions et leurs points de vue ont permis d'enrichir cette recherche et d'en améliorer la qualité.

De plus, je souhaite adresser une pensée toute particulière ma famille. Son soutien indéfectible, sa confiance, sa patience et ses encouragements m'ont accompagné tout au long de ce parcours et m'ont donné la force de mener ce projet à son terme. Elle a été une source constante de motivation et d'inspiration.

J'espère que ce mémoire apportera une contribution utile à la compréhension des stratégies de communication mises en œuvre par les organisations face aux fuites de données et qu'il pourra nourrir les réflexions de futurs étudiants, chercheurs et professionnels intéressés par cette thématique.

(L'IA générative a été utilisée comme assistant linguistique pour la reformulation et l'uniformisation stylistique de certains passages. L'ensemble du contenu, des choix théoriques et de l'analyse empirique est le produit de l'auteur.)

TABLE DES MATIÈRES

RÉSUMÉ **1**
REMERCIEMENTS **3**
INTRODUCTION **5**
PARTIE I — CADRE THÉORIQUE **7**
1. Communication externe et réputation organisationnelle 7
2. Communication de crise 13
3. Informatisation des organisations et sécurité des données 20
4. Fuite de données et stratégies de communication 23
5. Construction du modèle d'analyse et formulation des hypothèses 32
PARTIE II — RECHERCHE EMPIRIQUE **38**
6. Méthodologie de la recherche empirique 38
7. Analyse et résultats 46
CONCLUSION GÉNÉRALE **67**
BIBLIOGRAPHIE **70**
ANNEXES **75**
Annexe 1. Guide d'entretien 75
Annexe 2. Retranscriptions des entretiens 80
Déclaration sur l'honneur **97**

INTRODUCTION

Les organisations n'ont jamais été aussi dépendantes des données qu'elles collectent, traitent et stockent pour fonctionner. Cette dépendance croissante, conséquence directe de la transformation numérique, s'accompagne d'une exposition tout aussi croissante à un risque spécifique : la fuite de données. Qu'elle résulte d'une cyberattaque, d'une erreur humaine ou d'une faille technique, la fuite de données place l'organisation dans une situation paradoxale. Elle est à la fois victime d'un incident technique et responsable, aux yeux de ses parties prenantes, de la protection des informations qui lui avaient été confiées. Cette ambiguïté rend la communication qui suit un tel incident particulièrement délicate : comment rendre compte d'une défaillance sans achever de saper la confiance que l'on cherche précisément à préserver ?

Ce mémoire s'inscrit dans ce questionnement. Il part du constat que la fuite de données constitue une crise organisationnelle d'un type particulier, à la croisée de la cybersécurité, du management stratégique et de la communication. Contrairement à d'autres crises plus classiques, elle touche un actif immatériel — la donnée — dont la perte n'est pas toujours immédiatement visible ni quantifiable, mais dont les répercussions sur la réputation, l'image et la confiance des publics peuvent être considérables et durables. Face à ce type d'incident, les organisations disposent-elles de repères théoriques et pratiques suffisants pour communiquer efficacement ? C'est cette interrogation qui a guidé la question de recherche retenue pour ce travail : quelle stratégie de communication une entreprise met-elle en place auprès du grand public en cas de fuite de données ?

Pour y répondre, ce mémoire mobilise un ensemble de cadres théoriques issus des sciences de l'information et de la communication. La communication corporate et la notion de réputation organisationnelle constituent un premier ancrage, permettant de comprendre ce que les organisations cherchent à protéger. La communication de crise, et plus particulièrement deux théories de référence — la Situational Crisis Communication Theory (SCCT) de Coombs et l'Image Repair Theory de Benoit — offrent ensuite un cadre pour analyser les stratégies discursives mobilisées lorsque la réputation est mise à mal. Ces cadres sont enfin articulés à la littérature spécifique aux fuites de données, à la cybersécurité et à la réglementation applicable en matière de protection des données, notamment le Règlement général sur la protection des données (RGPD).

Cette articulation théorique débouche sur la construction d'un modèle d'analyse original, structuré autour de cinq dimensions — la temporalité de la communication, la stratégie

discursive adoptée, le canal utilisé, le public visé et le registre du message, ainsi que l'action corrective mise en œuvre — et sur quatre hypothèses de travail. Ce modèle est ensuite confronté au terrain à travers une démarche qualitative combinant des entretiens semi-directifs menés auprès de professionnels de la communication, de la sécurité informatique et de la gestion de crise, et l'analyse de cas réels de communication post-incident.

Ce mémoire se structure en deux grandes parties. La première partie propose le cadre théorique de la recherche : elle examine successivement la communication externe et la réputation organisationnelle, la communication de crise et ses théories de référence, la transformation numérique des organisations et les enjeux de sécurité des données, la fuite de données comme crise communicationnelle spécifique, avant de déboucher sur le modèle d'analyse et les hypothèses de travail. La seconde partie présente la recherche empirique : elle détaille la méthodologie retenue, puis expose et discute les résultats obtenus, avant de formuler, en conclusion générale, une réponse à la question de recherche ainsi que des recommandations pratiques à destination des organisations confrontées à une fuite de données.

PARTIE I — CADRE THÉORIQUE

La présente revue de littérature établit les fondements conceptuels et théoriques sur lesquels repose l'analyse des stratégies de communication déployées par les organisations à la suite d'une fuite de données. Elle se situe à l'intersection des sciences de l'information et de la communication, du management stratégique et des systèmes d'information. Cinq chapitres se succèdent de manière progressive : la communication externe et la réputation organisationnelle, la communication de crise et ses théories de référence, la transformation numérique des organisations et la sécurité des données, la fuite de données comme crise communicationnelle spécifique, et enfin la construction du modèle d'analyse et des hypothèses de travail.

Cette progression est à la fois thématique et logique. Le premier chapitre ancre l'objet d'étude dans la problématique de la réputation — le bien immatériel que les organisations cherchent à protéger. Le deuxième chapitre y ajoute la dimension de la crise, en mobilisant les deux théories dominantes du champ. Le troisième contextualise la montée en puissance des fuites de données dans le cadre de la transformation numérique. Le quatrième applique ces cadres au type de crise qui nous occupe. Le cinquième ferme la boucle en proposant un modèle opérationnel et des hypothèses testables.

1. Communication externe et réputation organisationnelle

Toute crise liée à une fuite de données touche d'abord à l'image, à la réputation et à la confiance. Ces trois actifs immatériels constituent le capital symbolique de l'organisation — un capital que des années de communication soigneuse ont contribué à bâtir, et qu'un incident peut mettre à mal en quelques heures. Comprendre leur construction, leur fragilité et les dynamiques qui les gouvernent est le préalable à toute réflexion sur les stratégies de communication de crise.

1.1 Définition et évolution de la communication externe

La communication externe désigne l'ensemble des pratiques par lesquelles une organisation s'adresse à des publics situés au-delà de ses frontières institutionnelles. Dans la tradition francophone, Libaert (2021) la définit comme « l'ensemble des actions et messages adressés à des publics extérieurs dans le but de construire et de maintenir une image favorable, de diffuser de l'information sur ses activités et de gérer ses relations avec son environnement ». Cette

définition souligne deux dimensions indissociables : l'information et le positionnement. Communiquer vers l'extérieur, c'est à la fois rendre compte de la réalité de l'organisation et construire une représentation souhaitée de cette réalité auprès de publics aux attentes multiples.

Cornelissen (2023) propose, dans son ouvrage Corporate Communication : A Guide to Theory and Practice, une formulation complémentaire et particulièrement éclairante : « Corporate communication is a management function that offers a framework for the effective coordination of all internal and external communication with the overall purpose of establishing and maintaining favourable reputations with stakeholder groups upon which the organization is dependent. » Trois éléments ressortent de cette définition : la dimension managériale de la communication, sa vocation à coordonner l'ensemble des messages de l'organisation, et sa finalité réputationnelle. Van Riel (1992) rejoint cette lecture en décrivant la communication corporate comme un instrument « par lequel toutes les formes de communication, internes et externes, sont harmonisées de la manière la plus efficace et la plus efficiente possible ».

Cornelissen (2023) retrace l'évolution de cette fonction au fil du temps. Jusqu'aux années 1970, les praticiens parlaient simplement de « relations publiques ». Le terme de communication corporate s'est imposé lorsque les parties prenantes — internes comme externes — ont commencé à réclamer davantage d'informations et de transparence. La fonction a alors intégré un éventail de disciplines spécialisées : design d'entreprise, publicité institutionnelle, communication interne, gestion des enjeux et des crises, relations avec les investisseurs et les médias, affaires publiques. Ce faisant, elle a changé de nature : d'instrument de diffusion, elle est devenue une fonction de coordination et de pilotage. Comme le résume Richard Edelman, cité par Cornelissen (2023) : « we used to be the tail on the dog, but now communication is the organizing principle behind many business decisions. » Pour Libaert et Mas (2022), la communication externe se distingue de la communication produit en ce qu'elle engage l'organisation en tant que personne morale : c'est l'entreprise qui parle d'elle-même, de ses valeurs, de sa mission.

Cette évolution est indissociable des transformations de l'environnement médiatique. Pendant longtemps, la communication externe se déployait selon un modèle unilatéral : l'organisation émettait, les publics recevaient. La montée des médias socionumériques — amorcée dès la fin des années 1990 et accélérée par l'essor des réseaux sociaux dans les années 2000 — a fondamentalement remis en cause ce modèle. L'organisation n'est plus seule à parler d'elle-même. Ses clients, ses employés, ses concurrents, les journalistes, les activistes numériques

participent tous à la construction de son image et de sa réputation. Cette polyphonie constitue à la fois une opportunité — en multipliant les canaux de diffusion — et un risque — en rendant plus difficile le contrôle des narratifs.

1.2 Image, réputation et confiance : un triptyque structurant

Trois notions structurent la communication externe : l'image, la réputation et la confiance. Elles sont étroitement liées, mais ne se confondent pas — et leur distinction est précieuse, notamment en situation de crise.

Libaert (2021) différencie la notoriété — le simple fait d'être connu — de l'image, définie comme « la représentation qualitative de l'entreprise auprès de différents publics, la manière dont elle est perçue ». L'image est dynamique, multiforme et varie selon les interlocuteurs. Une même organisation peut jouir d'une excellente image auprès de ses clients et d'une image dégradée auprès des médias, ou d'une image de marque forte et d'une image d'employeur contestée. Cette plasticité rend l'image à la fois plus facile à travailler — un acte de communication bien conduit peut en modifier la perception à court terme — et plus volatile.

Cornelissen (2023) introduit une distinction plus fine entre image et réputation. L'image est « the immediate set of associations of an individual in response to one or more signals or messages from or about a particular organization at a single point in time » — une réaction instantanée, sensible aux événements du moment, et qui peut varier selon les individus. La réputation, quant à elle, est « an individual's collective representation of past images of an organization established over time » — une construction sédimentée dans la durée, qui agrège les impressions successives. Cette distinction a des conséquences pratiques importantes : si un seul incident peut dégrader une image, la réputation résiste mieux aux chocs, mais se reconstruit aussi plus lentement une fois endommagée. Coombs (2007) la définit comme « une évaluation agrégée que les parties prenantes font sur la manière dont une organisation répond à leurs attentes, fondée sur ses comportements passés ».

Fombrun et Van Riel (2004, cités dans Cornelissen, 2023 et Coombs, 2007) qualifient la réputation d'actif immatériel précieux, un véritable « capital réputationnel » que l'organisation accumule au fil du temps. Ce capital fonctionne comme un amortisseur en période de crise : une entreprise bien réputée bénéficie du bénéfice du doute. Ses parties prenantes sont davantage enclines à traiter l'incident comme un accident isolé plutôt que comme une défaillance systémique. Coombs (2007) décrit ce mécanisme en des termes très clairs : une organisation

avec une réputation favorable subira moins de dommages réputationnels et rebondira plus rapidement, car elle dispose de davantage de capital réputationnel à « dépenser ». Ce concept est directement opérationnel dans notre analyse : les organisations qui jouissaient d'une bonne réputation avant une fuite de données bénéficient d'une marge communicationnelle que n'ont pas celles dont l'image était déjà dégradée.

Cornelissen (2023) identifie plusieurs attributs qui caractérisent les organisations aux réputations les plus solides : la visibilité de leurs valeurs, le caractère distinctif de leur positionnement, l'authenticité de leur identité, la transparence de leurs pratiques et la cohérence de leurs communications. Ces attributs se retrouvent dans les prescriptions de la littérature sur la communication de crise : l'authenticité, la transparence et la cohérence sont précisément les qualités que les parties prenantes attendent lorsqu'une organisation gère une fuite de données.

À l'extrémité la plus sévère du spectre réputationnel, Cornelissen (2023) décrit le risque de stigmate organisationnel : « a collective stakeholder group-specific perception that an organization possesses a fundamental, deep-seated flaw or quality which is demonstrated in repeated crisis or failures ». Ce stigmate conduit les parties prenantes à se déidentifier de l'organisation et parfois à agir activement contre elle. Il est particulièrement préoccupant pour les organisations dont la valeur proposée repose sur la confiance dans la gestion des données — banques, compagnies d'assurance, opérateurs de santé, plateformes numériques.

La confiance, troisième composante de ce triptyque, est définie par Loucif (2014) comme « une décision fondée à la fois sur des raisons rationnelles et des considérations émotionnelles ». McAllister (1995, cité dans Loucif, 2014) distingue la confiance cognitive — fondée sur un calcul de fiabilité et de compétence — de la confiance affective, construite par l'expérience relationnelle et l'attachement émotionnel. Une fuite de données touche simultanément ces deux registres : elle remet en cause la compétence technique de l'organisation (dimension cognitive), et elle trahit une relation construite dans le temps (dimension affective). La restauration de la confiance après une violation exige par conséquent des réponses qui s'adressent à ces deux niveaux.

1.3 Identité organisationnelle, alignement et authenticité

Cornelissen (2023), s'appuyant sur les travaux fondateurs de Birkigt et Stadler (1986), définit l'identité d'entreprise comme l'ensemble des éléments de présentation externe de l'organisation — son symbolisme, sa communication et le comportement de ses membres. Le modèle de Hatch

et Schultz, repris dans l'ouvrage, insiste sur la nécessité d'un alignement entre trois niveaux : la vision de la direction (ce que l'organisation aspire à être), la culture vécue par les salariés (ce qu'elle est en réalité de l'intérieur) et l'image perçue par les parties prenantes externes (ce qu'elles pensent qu'elle est). Tout écart significatif — un vision-culture gap (décalage entre la vision affichée et la culture interne) ou un image-culture gap (décalage entre l'image externe et la réalité interne) — crée des conditions propices à une crise de réputation.

Cornelissen (2023) formule cette mise en garde de façon directe : « if there are any outright discrepancies, or concerns about the organization not being true to its values, or not acting in character, this is picked up by the media and individual stakeholders, who will quickly organize for action and point out the lack of authenticity. » Dans le cas d'une fuite de données, cet écart entre les valeurs de protection de la vie privée affichées par l'organisation et la réalité de ses lacunes sécuritaires est immédiatement perceptible — et exploité.

L'authenticité est ainsi une notion centrale dans la communication de crise. Les parties prenantes n'attendent pas la perfection des organisations ; elles attendent la cohérence entre les actes et les mots. Une organisation qui a longtemps communiqué sur son engagement envers la protection des données et qui se révèle défaillante en la matière sera jugée d'autant plus sévèrement que le décalage est grand. À l'inverse, une organisation qui a construit sa réputation sur la transparence et l'honnêteté bénéficiera, lors d'une crise, d'une disposition positive de ses parties prenantes à lui accorder le bénéfice du doute.

Cette logique rejoint les réflexions de Libaert (2022), qui observe que la qualité de l'image institutionnelle préalable est le paramètre le plus déterminant dans la gestion d'une crise : « une entreprise possédant une bonne image globale a davantage de chances de surmonter une crise ». Il cite en illustration le cas de Coca-Cola, qui a traversé sans trop de séquelles une crise liée à la présence de dioxine dans certaines canettes (1999), malgré une communication de crise fortement contestée, précisément parce que son capital d'image était exceptionnel. À l'inverse, une entreprise dont l'image préalable est négative — ou perçue comme hypocrite — ne bénéficiera d'aucun filet de sécurité réputationnel en cas de crise.

1.4 Communication numérique et nouvelles dynamiques relationnelles

L'essor des médias socionumériques a profondément reconfiguré les modalités de la communication externe. Cornelissen (2023) parle d'un véritable « game-changer for corporate communication » : le modèle de commandement et de contrôle — dans lequel l'organisation

maîtrisait unilatéralement les messages — a laissé place à des échanges interactifs, multidirectionnels, parfois incontrôlables. Libaert (2021) le dit autrement : l'entreprise perd la maîtrise de son propre récit. La communication est désormais instantanée, et l'échange en est devenu le principe organisateur.

Catellani (2022) retrace l'évolution des médias socionumériques depuis le lancement de Facebook en 2004, jusqu'à l'émergence de YouTube, Twitter, Pinterest, Instagram et TikTok. Elle souligne que ces plateformes ont non seulement multiplié les canaux de communication, mais qu'elles ont fondamentalement transformé le rapport des publics à l'information. Les utilisateurs ne sont plus de simples récepteurs : ils produisent, commentent, partagent et détournent les contenus. Cette culture de la participation implique que les organisations doivent désormais penser leur communication comme un dialogue permanent plutôt que comme une diffusion unilatérale.

Catellani (2022) rappelle que les cinq indicateurs de gestion des relations publiques identifiés par Ledingham et Bruning (1998) — fiabilité (level of truth), transparence (openness), implication (involvement), investissement (investment) et engagement à long terme (commitment) — s'imposent plus que jamais comme des impératifs communicationnels dans l'environnement numérique. Ces cinq dimensions dessinent le profil d'une organisation communicante crédible et digne de confiance dans l'espace numérique. Cornelissen (2023) identifie enfin une tendance de fond structurante : le passage d'un paradigme de positionnement (où l'organisation cherche à occuper une place dans l'esprit des publics) à celui de l'engagement des parties prenantes (où l'organisation cherche à construire des relations dialogiques). Interactivité, authenticité, transparence — des attentes qui pèsent de tout leur poids lors d'une gestion de crise, et qui rendent les stratégies défensives ou technicistes particulièrement inadaptées dans un contexte de fuite de données.

Cette transformation des dynamiques communicationnelles a des implications directes pour la communication de crise. D'une part, les crises se propagent plus rapidement et plus largement que jamais : une fuite de données révélée par un seul tweet peut déclencher en quelques heures une tempête médiatique mondiale. D'autre part, les organisations disposent désormais de canaux directs pour s'adresser à leurs parties prenantes sans intermédiaire médiatique. Cette double réalité — accélération des crises et opportunité de réponse directe — constitue l'un des enjeux centraux de la communication de crise contemporaine.

2. Communication de crise

Ce deuxième chapitre examine les théories et les concepts propres à la communication de crise. C'est le cœur du cadre théorique : toute fuite de données est d'abord une crise communicationnelle, qui appelle une réponse stratégique, rapide et adaptée. Nous procèderons en trois temps : définition et caractérisation de la crise, articulation entre communication de crise et réputation, puis exposition des deux théories structurantes.

2.1 Définition et caractéristiques de la crise organisationnelle

La notion de crise organisationnelle a fait l'objet de nombreuses définitions académiques et pratiques qui, loin d'être redondantes, éclairent différentes facettes du phénomène. Dans la tradition francophone, Libaert (2022) reprend la définition de Lerbinger : la crise est « un événement inattendu mettant en péril la réputation et le fonctionnement d'une organisation ». Deux termes y sont déterminants : l'effet de surprise, et l'accent mis sur la réputation — signalant que la crise est fondamentalement un phénomène de perception autant qu'un événement objectif.

Cette définition doit cependant être nuancée. Libaert (2022) souligne que les crises sont de moins en moins imprévisibles : les retours d'expérience postérieurs aux crises indiquent majoritairement que l'événement avait été pressenti ou aurait pu l'être. Roux-Dufort (2003), cité dans Libaert (2022), va plus loin : « les crises ne sont pas des événements mais des processus qui se développent dans le temps et l'espace. » Cette perspective processuelle est précieuse pour les fuites de données, qui résultent souvent d'une accumulation de vulnérabilités non traitées plutôt que d'une cause unique et soudaine.

Cornelissen (2023) propose une formulation plus opérationnelle : « Broadly speaking, a crisis is defined as an event or issue that requires decisive and immediate action from an organization. » Coombs (2007) la caractérise comme « a sudden and unexpected event that threatens to disrupt an organization's operations and poses both a financial and a reputational threat. » Ces définitions convergent : la crise est fondamentalement une menace — réputationnelle autant qu'opérationnelle — qui exige une réponse communicationnelle rapide et appropriée.

Libaert (2022) identifie cinq caractéristiques structurantes communes à toutes les crises, indépendamment de leur nature. La première est l'intrusion de nouveaux acteurs : des interlocuteurs inattendus — pouvoirs publics, associations, militants, journalistes d'investigation — s'expriment, exigent des explications et contribuent à définir les termes du

débat. La deuxième est la saturation des canaux de communication : l'organisation est submergée de demandes, au point que ses capacités de réponse sont dépassées. La troisième est l'importance des enjeux : la survie même de l'organisation peut être menacée. La quatrième est l'accélération du temps : les réseaux sociaux créent une pression temporelle extrême qui oblige l'organisation à communiquer avant même d'avoir une image complète de la situation. La cinquième est la montée des incertitudes : les informations disponibles sont partielles, contradictoires et changeantes.

Ces cinq caractéristiques se retrouvent de manière particulièrement marquée dans les crises liées aux fuites de données. L'intrusion de nouveaux acteurs y est amplifiée par les réseaux sociaux : des experts en cybersécurité, des journalistes spécialisés, des associations de protection des données personnelles et des régulateurs prennent rapidement la parole. La saturation des canaux est exacerbée par la multiplicité des plateformes. L'accélération du temps est maximale. Et les incertitudes sur l'étendue réelle de la fuite, les données compromises et les responsabilités peuvent persister pendant des semaines.

Cornelissen (2023), s'appuyant sur Coombs (2007), propose une classification des crises en quatre types selon deux dimensions — interne/externe et intentionnel/non-intentionnel. Le faux pas (faux pas) survient lorsque des décisions organisationnelles légitimes sont transformées en crise par un acteur extérieur. L'accident (accident) est non intentionnel et survient dans le cours normal des opérations. La transgression (transgression) désigne des actions intentionnelles exposant sciemment les parties prenantes à un risque. L'agression (agression) renvoie à des actes intentionnels commis par des acteurs externes. Cette taxonomie est directement applicable aux fuites de données : une violation causée par une cyberattaque externe relève de l'agression — les attributions de responsabilité envers l'organisation sont minimales. Une violation due à des négligences sécuritaires connues relève de la transgression — elles sont maximales. Cette distinction est capitale pour la communication : elle détermine quel type de stratégie est le plus approprié.

Robert et Verpeaux (1991, cités dans Libaert, 2022) modélisent le déroulement des crises en quatre phases. La phase préliminaire est celle des signaux d'alerte — rumeurs, plaintes éparses, commentaires négatifs sur les réseaux sociaux. C'est « à ce stade que tout se joue », note Libaert (2022) : si l'organisation dispose d'un dispositif de veille stratégique, elle peut parfois juguler la crise avant même son émergence. La phase aiguë correspond à l'explosion médiatique : l'événement est rendu public et la montée en intensité est souvent très rapide. La phase

chronique voit progressivement se réduire l'attention médiatique, selon une logique de renouvellement de l'agenda. Enfin, la phase de cicatrisation voit la crise disparaître de l'espace médiatique — mais jamais totalement de la mémoire collective. Internet conserve en effet une trace indélébile des crises, et les moteurs de recherche permettent de retrouver instantanément des articles datant de plusieurs années. Cette résilience mémorielle de l'espace numérique est une réalité que les organisations ne peuvent ignorer. Cornelissen (2023) y ajoute une étape fondamentale en amont : l'anticipation.

2.2 Communication de crise et réputation : une relation bidirectionnelle

La relation entre communication de crise et réputation est bidirectionnelle et complexe. D'un côté, la réputation préalable conditionne la capacité de l'organisation à surmonter la crise. De l'autre, la communication de crise détermine l'ampleur des dégâts réputationnels.

Cornelissen (2023) montre que le capital réputationnel préalablement accumulé peut « buffer or shield the company from a crisis having a lasting negative impact ». La crise érode ce capital, mais une organisation bien ancrée dans la confiance de ses parties prenantes peut en absorber le choc. Il identifie deux étapes essentielles dans la réponse communicationnelle : informer les parties directement affectées sur ce qui s'est passé et sur les mesures prises, puis communiquer plus largement sur la responsabilité de l'organisation et sur ses engagements. Coombs (2007) formule ce principe de manière prescriptive : le premier devoir communicationnel d'une organisation en crise est d'informer les parties prenantes sur ce qu'elles doivent faire pour se protéger (instructing information) et de les aider à gérer l'incertitude psychologique créée par la crise (adjusting information). Ce n'est qu'une fois ces obligations remplies que l'organisation peut se tourner vers la restauration de sa réputation.

Libaert (2022) rappelle cependant que la communication de crise a des limites face aux incidents les plus graves. Confrontée à des catastrophes d'une ampleur exceptionnelle, la communication ne peut que réduire certaines tensions, rarement surmonter l'événement. La qualité de l'image préalable reste le paramètre le plus déterminant — c'est elle qui accorde ou non le bénéfice du doute. Il illustre ce constat par un exemple saisissant : celui de Zinedine Zidane lors de la finale de la Coupe du monde 2006, dont la réputation exceptionnelle lui a permis de traverser sa crise personnelle sans voir son image définitivement entachée — une latitude qui n'aurait pas été accordée à un joueur moins emblématique.

La communication de crise est également une « branche de la communication globale », note Libaert (2022) : elle ne saurait être efficace si l'organisation ne dispose pas d'une stratégie de communication d'ensemble. Les messages de crise s'appuient sur des valeurs, des cibles et des positionnements construits en amont. Une organisation qui n'a jamais clairement exprimé ses engagements en matière de protection des données sera dans une position communicationnelle fragile lorsqu'une fuite surviendra.

Roux-Dufort (2003), cité dans Libaert (2022), insiste par ailleurs sur l'écart de perception entre l'organisation et ses parties prenantes externes comme principal déterminant de la communication de crise. Si l'organisation minimise la gravité de la situation alors que ses publics la perçoivent comme très sérieuse, cet espace critique ne peut que se creuser. Ce n'est que par une communication proactive, transparente et empathique que cet écart peut être comblé.

2.3 Théories de la communication de crise

2.3.1 La Situational Crisis Communication Theory (SCCT)

La Situational Crisis Communication Theory (SCCT), développée par W. Timothy Coombs à partir des années 1990 et formalisée en 2007, est aujourd'hui l'un des cadres les plus utilisés en recherche empirique sur la communication de crise. Sa force principale tient à son ancrage dans une méthodologie expérimentale plutôt que dans l'étude de cas, ce qui lui confère une robustesse empirique que les approches narratives ne possèdent pas.

La SCCT s'appuie sur la théorie de l'attribution (Weiner, 1985, 1986, 2006, cités dans Coombs, 2007) : face à un événement négatif, les individus cherchent naturellement à en identifier les causes et à attribuer des responsabilités. Ces attributions génèrent des réactions émotionnelles — principalement la colère (lorsque la responsabilité est forte) et la sympathie (lorsqu'elle est faible) — qui influencent ensuite les comportements : boycott, diffusion de commentaires négatifs, soutien ou abandon de l'organisation.

La SCCT identifie trois facteurs déterminant le niveau de menace réputationnelle. Le premier est la responsabilité initiale de la crise (crisis responsibility), qui correspond au degré auquel les parties prenantes attribuent la crise à l'organisation. Elle est déterminée par le type de crise. Le deuxième facteur est l'historique de crises (crisis history) : une organisation ayant déjà subi une crise similaire sera davantage tenue pour responsable de la nouvelle. Le troisième est la réputation relationnelle préalable (prior relational reputation) : une organisation qui a traité ses

parties prenantes de manière défavorable dans d'autres contextes verra ses attributions de responsabilité renforcées.

En fonction de ces facteurs, Coombs (2007) regroupe les crises en trois clusters. Le cluster victimaire (victim cluster) comprend les situations dans lesquelles l'organisation est elle-même victime — catastrophe naturelle, sabotage externe, rumeur infondée. Les attributions de responsabilité y sont très faibles. Le cluster accidentel (accidental cluster) comprend des événements non intentionnels survenus dans le cours normal des opérations — incident technique, accident de fabrication. Les attributions sont minimales. Le cluster intentionnel (intentional cluster) comprend des situations dans lesquelles l'organisation est perçue comme ayant agi de manière délibérément négligente ou malveillante — misdeed, violation de normes. Les attributions de responsabilité y sont maximales.

À chacun de ces clusters correspondent des familles de stratégies de réponse. Les stratégies de déni (deny) cherchent à séparer l'organisation de la crise : déni pur, contre-attaque, désignation d'un bouc émissaire. Elles sont appropriées lorsque la responsabilité est nulle. Les stratégies d'atténuation (diminish) cherchent à réduire la perception de la crise sans nier totalement toute responsabilité : excuse, justification, minimisation. Elles sont appropriées pour les crises accidentelles. Les stratégies de reconstruction (rebuild) cherchent à rétablir la réputation en prenant en charge les victimes et en reconnaissant la responsabilité : compensation, excuses complètes, action corrective. Elles sont nécessaires pour les crises intentionnelles. S'y ajoutent des stratégies de renforcement (bolstering) utilisées en complément : rappel des bons antécédents, valorisation de l'aide fournie aux parties prenantes.

Coombs (2007) formule un principe fondamental qui prime sur toute autre considération : « The first priority in any crisis is to protect stakeholders from harm, not to protect the reputation. » Ce principe éthique est fondateur de la SCCT. Il signifie que la communication de crise doit d'abord servir les victimes — leur fournir les informations dont elles ont besoin pour se protéger — avant de servir les intérêts réputationnels de l'organisation. Ce principe est d'autant plus pertinent pour les fuites de données que les victimes peuvent être des millions d'individus dont les données personnelles ont été compromises.

Coombs (2014) apporte un complément important à ce cadre en documentant l'effet de la temporalité sur l'efficacité des stratégies de communication. Il confirme notamment la valeur du stealing thunder — la divulgation proactive de la crise par l'organisation elle-même — comme stratégie réduisant significativement les dommages réputationnels. Il met également en

garde contre deux erreurs stratégiques majeures : le scapegoating, qui génère des réactions négatives car les parties prenantes attendent de l'organisation qu'elle assume la responsabilité ultime de ses produits et services, et le déni suivi d'une révélation de responsabilité, qui amplifie considérablement les dommages en créant ce que Frandsen et Johansen (2010) appellent une « double crise ».

Claeys, Cauberghe et Vyncke (2010), dans une étude expérimentale portant sur 316 consommateurs, ont fourni une confirmation empirique des prescriptions de la SCCT : les crises préventables ont les effets les plus négatifs sur la réputation, et les stratégies de reconstruction conduisent aux meilleures restaurations réputationnelles. Ces résultats renforcent la pertinence de la SCCT comme cadre analytique pour les fuites de données, qui sont fréquemment perçues comme préventables.

Kim, Avery et Laricy (2009), dans leur revue systématique de 51 articles publiés entre 1991 et 2009, confirment que la SCCT constitue l'un des deux paradigmes dominants de la recherche en communication de crise — l'autre étant la théorie de Benoit. Ils soulignent cependant des limites importantes : la SCCT repose sur des populations d'étudiants dans des contextes expérimentaux artificiels, ce qui peut limiter sa validité externe. Ces limites nous conduisent à la mobiliser non comme une théorie prescriptive universelle, mais comme un cadre analytique dont les propositions doivent être nuancées à la lumière des contextes spécifiques.

2.3.2 L'Image Repair Theory de Benoit

La théorie de la réparation de l'image (Image Repair Theory), développée par William L. Benoit à partir des années 1990 et formalisée en 1997, constitue le second cadre théorique de référence. Là où la SCCT raisonne en termes de situation et de stratégie globale, Benoit s'attache à la rhétorique des messages — aux choix discursifs opérés par les organisations pour défendre et restaurer leur image.

Benoit (1997) part d'un constat simple mais fondateur : l'image est essentielle aux organisations, et lorsqu'une crise la menace, elles disposent d'un répertoire de stratégies rhétoriques pour la restaurer. Deux conditions sont nécessaires pour que ces stratégies soient activées : l'acte doit être jugé offensant par les parties prenantes, et il doit être attribué à l'organisation concernée. Si l'une ou l'autre de ces conditions fait défaut, la réparation d'image devient inutile.

Benoit (1997) répertorie cinq grandes catégories de stratégies. Le déni (denial) cherche à réfuter toute implication dans l'acte incriminé, soit par déni simple, soit en désignant un tiers

responsable. L'évasion de responsabilité (evading responsibility) cherche à minimiser la responsabilité sans la nier totalement : en invoquant la provocation, le manque d'information, l'accident ou les bonnes intentions. La réduction de l'offensivité (reducing offensiveness) cherche à atténuer la perception négative de l'acte : en rappelant les bons antécédents (bolstering), en minimisant l'ampleur des dommages (minimization), en attaquant les accusateurs (attacking accuser), en proposant une compensation, ou encore en transcendant l'incident dans un cadre plus favorable (transcendence). L'action corrective (corrective action) désigne les mesures prises pour remédier aux problèmes et prévenir leur récurrence. La mortification (mortification), enfin, consiste en la reconnaissance complète de la faute accompagnée d'une demande de pardon.

Ces cinq catégories forment un continuum qui va des stratégies les plus défensives (le déni) aux stratégies les plus accommodatives (la mortification). La théorie de Benoit ne prescrit pas de stratégie universellement supérieure, mais souligne que le choix doit être cohérent avec la gravité de l'acte incriminé et le niveau d'attribution de responsabilité. Une stratégie de déni appliquée à une situation de forte responsabilité organisationnelle sera non seulement inefficace mais contre-productive.

Cornelissen (2023) articule les apports de Benoit avec la SCCT et la communication corporate en soulignant le principe de proportionnalité entre responsabilité perçue et accommodativité de la réponse. Il intègre les stratégies de Benoit dans un cadre plus large en les regroupant en cinq familles : non-existence (denial, clarification, attack), distanciation (excuse, downplay), association (bolstering, transcendence), souffrance (victimization) et acceptation (full apology, remediation, repentance, rectification). Cette reclassification facilite l'opérationnalisation analytique des stratégies dans le cadre de notre étude.

L'articulation entre la SCCT et l'Image Repair Theory est féconde. La SCCT fournit un cadre pour évaluer la situation et prescrire une famille de stratégies ; Benoit fournit les outils rhétoriques pour les mettre en œuvre. Les deux approches convergent sur un point central : l'action corrective est un levier indispensable de restauration de l'image et de la confiance. Elle ne se limite pas à la communication : elle implique des mesures tangibles, visibles et vérifiables qui montrent que l'organisation a non seulement compris ce qui s'est passé, mais qu'elle a agi pour l'empêcher de se reproduire.

3. Informatisation des organisations et sécurité des données

Ce troisième chapitre situe les fuites de données dans leur contexte structurel : la transformation numérique des organisations. Il s'agit de comprendre pourquoi ces incidents sont devenus une forme récurrente de crise organisationnelle, et quelles contraintes légales en découlent pour la communication.

3.1 Digitalisation et dépendance aux données

La transformation numérique est l'un des phénomènes les plus marquants des trois dernières décennies. Elle a profondément reconfiguré les modèles économiques, les processus opérationnels et les relations entre les organisations et leurs parties prenantes. Bharadwaj, El Sawy, Pavlou et Venkatraman (2013) soulignent que les technologies numériques « transforment fondamentalement les stratégies d'entreprise, les processus d'affaires, les capacités des entreprises, les produits et services, et les principales relations inter-firmes dans les réseaux d'affaires étendus ». Ces auteurs proposent le concept de digital business strategy pour désigner la fusion entre stratégie informatique et stratégie commerciale : l'infrastructure numérique n'est plus un simple outil d'appui, mais le substrat même de l'activité organisationnelle.

Cette dépendance numérique se manifeste à travers la collecte et le traitement de volumes considérables de données personnelles. Les organisations de tous secteurs — commerce, santé, finance, administration — ont fait des données un actif stratégique central. Elles les utilisent pour personnaliser leurs offres, optimiser leurs processus, prédire les comportements de leurs clients et développer de nouveaux services. Cette accumulation de données personnelles crée cependant une responsabilité proportionnelle : plus les données collectées sont sensibles et nombreuses, plus les conséquences d'une fuite sont graves.

Cornelissen (2023) observe que la transformation numérique a également transformé les attentes des parties prenantes : elles sont désormais beaucoup plus actives dans l'expression de leurs exigences, et s'organisent rapidement « at scale » lorsqu'elles estiment que leurs droits sont violés. Cette capacité d'organisation collective — amplifiée par les réseaux sociaux — est l'un des facteurs qui rendent les fuites de données particulièrement redoutables sur le plan réputationnel.

La dépendance aux systèmes d'information crée par ailleurs une vulnérabilité structurelle. Bharadwaj et al. (2013) notent que plus les organisations intègrent profondément les technologies numériques dans leurs opérations, plus les conséquences d'une défaillance ou

d'une intrusion sont sévères. Cette observation est directement pertinente pour notre sujet : une organisation dont l'ensemble des opérations repose sur des systèmes d'information interconnectés sera non seulement plus exposée aux fuites de données, mais sera aussi plus impactée si une fuite survient.

3.2 Cybersécurité et protection des données : enjeux stratégiques

Les cybermenaces sont aujourd'hui décrites comme « parmi les dangers de sécurité nationale les plus graves » (The White House, 2015, cité dans Romanosky, 2016). Cette formulation, qui peut sembler hyperbolique, reflète la réalité des enjeux : les attaques informatiques touchent indifféremment les entreprises, les hôpitaux, les administrations et les infrastructures critiques, avec des conséquences qui dépassent largement le seul périmètre des victimes directes.

Romanosky (2016), dans une analyse empirique de plus de 12 000 événements cybernétiques, apporte un résultat nuancé qui mérite d'être mentionné : les coûts financiers directs d'une violation représentent en moyenne 0,4 % des revenus annuels — relativement peu comparé aux coûts de certaines autres crises. Mais ce chiffre ne reflète pas l'ensemble des conséquences. Les effets sur la réputation, la confiance des consommateurs et les relations avec les partenaires sont bien plus sévères et durables. Romanosky (2016) distingue ainsi les coûts directs (notification, remédiation technique, poursuites judiciaires) des coûts indirects (perte de clients, dégradation de la réputation, érosion de la confiance).

Martin, Borah et Palmatier (2017) documentent l'existence d'effets de débordement (spillover effects) particulièrement importants dans le cas des fuites de données : des clients non directement affectés par la violation révisent à la baisse leur évaluation de la compétence et de l'intégrité de l'organisation. Ce mécanisme amplifie considérablement l'impact réputationnel d'une fuite, en touchant bien au-delà du cercle des victimes directes. Deux leviers stratégiques atténuent ces effets : la transparence sur les pratiques de gestion des données, et le contrôle offert aux clients sur leurs préférences de partage d'information. Ces deux leviers correspondent précisément à des choix de communication — ce qui confirme le rôle central de la communication dans la gestion des conséquences d'une fuite.

Goode, Hoehle, Venkatesh et Brown (2017), dans leur étude longitudinale sur le cas Sony PlayStation Network, montrent que la compensation offerte aux utilisateurs après une violation exerce un effet positif sur la confiance post-crise — à condition que la nature de la compensation corresponde aux attentes des parties prenantes. Ce résultat nuancé est important:

une compensation perçue comme insuffisante ou inadaptée peut être plus dommageable qu'une absence de compensation, en signalant que l'organisation ne comprend pas vraiment l'étendue du préjudice subi par ses clients.

Ces différentes études convergent vers une conclusion commune : les fuites de données ne sont pas seulement des incidents techniques. Elles sont des événements sociaux et communicationnels dont les conséquences réputationnelles dépassent largement les coûts financiers directs. La communication — transparente, rapide, empathique et orientée vers l'action — est un déterminant majeur de la capacité des organisations à limiter ces conséquences.

3.3 Le RGPD : contraintes légales et implications communicationnelles

L'adoption du Règlement Général sur la Protection des Données (RGPD) par le Parlement européen en mai 2016, entré en vigueur en mai 2018, marque un tournant réglementaire majeur dans le paysage de la protection des données personnelles. Tikkinen-Piri, Rohunen et Markkula (2018) analysent ses implications pour les entreprises collectant des données personnelles : le RGPD vise à renforcer la protection des individus en clarifiant les droits des personnes concernées et en précisant les obligations des responsables de traitement.

Du point de vue de la communication de crise, le RGPD introduit des obligations de notification aux conséquences directes et importantes. L'article 33 impose la notification à l'autorité de contrôle compétente (en France, la CNIL) dans les 72 heures suivant la prise de connaissance de la violation, même si toutes les informations ne sont pas encore disponibles. L'article 34 impose la notification directe aux personnes concernées lorsque la violation est susceptible d'engendrer un risque élevé pour leurs droits et libertés. Ces obligations créent une pression temporelle considérable sur les organisations confrontées à une fuite, les obligeant à communiquer rapidement même en l'absence d'informations complètes.

Paradoxalement, ces contraintes légales s'alignent sur les recommandations académiques de transparence et de rapidité. En obligeant les organisations à communiquer dans les 72 heures, le RGPD les contraint à adopter une posture de proactivité communicationnelle qui, selon la littérature, est la plus efficace pour limiter les dégâts réputationnels. En ce sens, la réglementation européenne crée un alignement entre impératifs légaux et bonnes pratiques communicationnelles.

Au-delà des obligations techniques, le RGPD institutionnalise la protection de la vie privée comme droit fondamental. L'article 8 de la Charte des droits fondamentaux de l'Union européenne, sur lequel s'appuie le RGPD, consacre la protection des données à caractère personnel comme un droit fondamental de chaque personne. Cette élévation juridique a des conséquences symboliques importantes : toute fuite de données est désormais perçue non seulement comme une défaillance technique, mais comme la violation d'un droit fondamental. Cette évolution accroît considérablement la charge symbolique et réputationnelle de ce type d'incidents.

Cette dimension réglementaire crée enfin une obligation de preuve et de traçabilité qui dépasse la seule communication. Les organisations doivent être en mesure de documenter non seulement leur réponse à la fuite, mais aussi les mesures de prévention mises en place et les actions correctives entreprises. Cette exigence de documentation s'articule directement avec les prescriptions de la littérature sur l'action corrective et la reconstruction de la confiance.

4. Fuite de données et stratégies de communication

Ce quatrième chapitre est le plus directement articulé à notre question de recherche. Il applique les cadres théoriques développés dans les chapitres précédents au contexte spécifique des fuites de données — en examinant leurs caractéristiques propres en tant que crises organisationnelles, puis les stratégies communicationnelles que la littérature identifie comme pertinentes.

4.1 Définition et spécificités d'une fuite de données

La fuite de données (data breach) est définie par le RGPD (Règlement UE 2016/679, article 4, §12) comme « une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données ». Cette définition couvre un spectre large d'incidents — de l'envoi accidentel d'un fichier au mauvais destinataire à une cyberattaque sophistiquée compromettant des millions de dossiers.

Romanosky (2016) affine cette définition en distinguant quatre catégories d'incidents cybernétiques : les violations de données proprement dites (data breaches), les incidents de sécurité (security incidents), les violations de la vie privée (privacy violations) et les crimes de

phishing. Cette distinction est utile pour la communication : chaque catégorie implique des niveaux différents de responsabilité organisationnelle et appelle des stratégies communicationnelles différentes.

Dans la classification de Cornelissen (2023), adaptée des travaux de Coombs (2007), les fuites de données relèvent de l'accident lorsqu'elles résultent d'erreurs humaines non intentionnelles — un employé qui perd un ordinateur portable non chiffré, par exemple —, et de la transgression lorsque l'organisation est jugée avoir sciemment négligé sa responsabilité — en maintenant des systèmes de sécurité insuffisants malgré des signaux d'alerte répétés. Cette distinction est capitale pour la communication : une fuite-accident appelle des stratégies de distanciation modérées, tandis qu'une fuite-transgression exige des stratégies d'acceptation pleine.

Syed (2020), dans son étude appliquant la SCCT à la violation Home Depot de 2014, identifie trois cadres (frames) interprétatifs mobilisés par le public sur Twitter : le cadre intentionnel, le cadre accidentel et le cadre victimaire. Elle montre que le cadre intentionnel génère les attributions de responsabilité les plus fortes et les réactions émotionnelles les plus intenses — colère, dégoût. Le cadre victimaire, à l'inverse, accorde davantage de latitude communicationnelle à l'organisation. Ces résultats soulignent l'importance du framing dans la communication de crise : l'organisation n'est pas passive face au cadrage de la crise, elle peut — et doit — tenter d'influencer la manière dont l'incident est interprété par ses parties prenantes.

Les fuites de données présentent trois spécificités structurelles par rapport aux autres crises organisationnelles. D'abord, leur nature intrinsèquement numérique implique qu'elles surgissent et se propagent dans l'environnement digital avant même que les médias traditionnels n'en prennent connaissance. Ensuite, leur temporalité peut être décalée : une fuite peut rester indétectée pendant des mois — le cas Yahoo, dont la violation de 2013 n'a été révélée qu'en 2016, en est l'illustration la plus marquante. Enfin, la portée potentiellement massive de ces incidents amplifie considérablement leurs effets réputationnels : une fuite touchant des millions d'individus mobilise une opinion publique bien plus large qu'un incident isolé.

4.2 Impacts réputationnels et perte de confiance

Les conséquences réputationnelles des fuites de données sont solidement documentées dans la littérature empirique. Romanosky (2016) montre que si les coûts financiers directs restent modestes en proportion des revenus, les effets sur la réputation et la confiance sont durables et

plus sévères. Cette asymétrie entre impact financier direct et impact réputationnel est caractéristique des crises de données : elles ne menacent pas directement les actifs physiques de l'organisation, mais attaquent sa réputation — son capital le plus précieux et le plus difficile à reconstruire.

Martin et al. (2017) distinguent deux types de conséquences réputationnelles. Les effets directs touchent les clients ayant eu leurs données compromises : ils réduisent leur confiance dans l'organisation, diminuent leurs achats et peuvent résilier leur relation commerciale. Les effets de débordement (spillover effects) touchent des clients non directement victimes mais qui, ayant pris connaissance de la fuite, révisent à la baisse leur évaluation de la compétence et de l'intégrité de l'organisation. Ces effets de débordement sont particulièrement importants dans les cas médiatisés, car ils transforment un incident touchant un sous-ensemble de clients en crise de réputation totale.

Sur les réseaux sociaux, ces effets se renforcent mutuellement. Syed (2020) montre que les attributions de responsabilité et les émotions négatives s'auto-amplifient : chaque publication négative accroît la probabilité de nouvelles publications négatives. Ce phénomène d'amplification en cascade est caractéristique des crises numériques : une fois enclenché, il est très difficile à arrêter par la seule communication. Cornelissen (2023) attire l'attention sur le risque de stigmatisation réputationnelle en cas de gestion défaillante ou de crises répétées — un stigmate dont il est extrêmement difficile de se défaire.

La perte de confiance est sans doute la conséquence la plus profonde et la plus durable d'une fuite de données. Loucif (2014) rappelle que la confiance repose sur des bases à la fois cognitives et affectives, simultanément ébranlées par une fuite. La confiance cognitive — fondée sur la croyance en la compétence et la fiabilité de l'organisation — est directement mise en cause : la fuite démontre une incapacité à protéger les données confiées. La confiance affective — fondée sur l'expérience relationnelle et l'attachement émotionnel — est trahie : la relation de confiance construite dans le temps est violée.

Goode et al. (2017), sur le cas Sony PlayStation Network, montrent que la compensation est un levier significatif de restauration de la confiance, à condition d'être bien calibrée. Ces résultats montrent que la confiance post-crise ne se restaure pas seulement par les mots : elle exige des actes concrets, visibles et cohérents. Gillespie et Dietz (2009) proposent un modèle de réparation de la confiance en quatre étapes : reconnaissance de la violation et de ses impacts, explication des causes, réforme démonstrative et preuves tangibles de changement. Cette

séquence — reconnaître, expliquer, agir, prouver — est robuste et convergente avec les cadres de la SCCT et de l'Image Repair Theory.

4.3 Réactions du public et des médias : mécanismes d'attribution

Les réactions des publics face aux fuites de données sont largement conditionnées par la façon dont la crise est encadrée et communiquée. Syed (2020) observe que la colère et le dégoût sont les réactions dominantes sur les réseaux sociaux — mais que la sympathie peut, dans le cadre victimaire, atténuer significativement les attributions de responsabilité. Ce résultat suggère que l'organisation a intérêt à mettre en avant sa propre victimisation (notamment dans les cas de cyberattaque externe) pour déplacer le cadrage de la crise.

Jin, Liu et Austin (2014), à travers le modèle SMCC (Social-Mediated Crisis Communication Model), montrent que lorsque la crise est d'origine interne, les publics préfèrent recevoir l'information directement de l'organisation concernée plutôt que d'une tierce partie. Ce résultat plaide pour une prise de parole proactive et directe : l'organisation doit être la première à informer, non pas parce que la loi l'y oblige (même si c'est souvent le cas), mais parce que cela correspond à l'attente des publics.

Cornelissen (2023) insiste sur le contrôle de l'information comme impératif communicationnel : « the key to effective crisis communication is to maintain effective control over the release of information and to ensure that no unauthorized information or potentially damaging rumours are allowed to circulate. » Ce principe se heurte cependant à la réalité des environnements numériques, dans lesquels l'information circule à une vitesse que les organisations ne peuvent contrôler. La solution n'est pas de chercher à bloquer l'information — ce qui est à la fois impossible et contre-productif — mais de devancer les rumeurs en communiquant de manière proactive et transparente.

Lee (2004) apporte un résultat contre-intuitif mais solidement documenté : la stratégie du « no comment » génère davantage de méfiance que la minimisation. Le silence n'est pas une posture neutre — il est perçu comme une forme d'aveu, voire de mépris. Cette observation est cohérente avec les réflexions de Libaert (2022) sur l'écart de perception : une organisation silencieuse laisse le champ libre à d'autres acteurs pour définir la crise à sa place.

4.4 Transparence et rapidité : le principe du stealing thunder

Transparence et rapidité : ce sont les deux impératifs les plus solidement documentés dans la littérature sur la communication de crise liée aux fuites de données. L'adage « tell it all and tell it fast » (Dillenschneider & Hyde, 1985, cités dans Arpan & Roskos-Ewoldsen, 2005) résume cette double injonction. Sur le plan de la transparence, Martin et al. (2017) la confirment empiriquement : la communication transparente sur les pratiques de gestion des données atténue significativement les effets négatifs d'une violation.

Catellani (2022) place la transparence au cœur des impératifs communicationnels dans l'environnement numérique : « L'authenticité et le parler vrai ne doivent pas être une tendance épisodique mais devenir la norme. » Elle rappelle que les publics numériques « réclament de la confiance, n'acceptent ni le mensonge, ni la dissimulation et attendent des organisations qu'elles disent la vérité, qu'elles annoncent ce qu'elles ont l'intention de faire et qu'elles fassent effectivement ce qu'elles ont au préalable annoncé ». Ces attentes sont particulièrement intenses lorsque les données personnelles des utilisateurs sont en jeu.

Sur le plan de la rapidité, le concept de "stealing thunder" désigne la stratégie par laquelle une organisation divulgue elle-même l'existence d'une crise avant que les médias ou d'autres acteurs ne le fassent. Arpan et Roskos-Ewoldsen (2005) l'ont démontré expérimentalement : cette auto-divulgation proactive génère des évaluations de crédibilité significativement plus élevées et une perception moins sévère de la crise. Lorsque l'organisation prend l'initiative de la révélation, les individus lui attribuent des motivations positives — honnêteté, sens des responsabilités — ce qui atténue les attributions négatives. Coombs (2014) confirme ce résultat dans une série d'études : l'organisation divulgatrice subit significativement moins de dommages réputationnels.

Le mécanisme psychologique qui sous-tend le stealing thunder est cohérent avec la théorie de l'attribution. Une organisation qui révèle elle-même une défaillance montre qu'elle a les valeurs d'honnêteté que ses parties prenantes attendent d'elle. À l'inverse, une organisation dont la fuite est révélée par un journaliste ou un lanceur d'alerte est perçue comme ayant cherché à dissimuler l'incident — ce qui génère une attribution d'intentionnalité négative qui amplifie considérablement les dommages réputationnels.

Il convient cependant de nuancer la prescription de rapidité absolue. Coombs (2014) reconnaît une tension entre vitesse et précision : communiquer trop vite, avec des informations incomplètes ou inexactes, peut exacerber la crise plutôt que la contenir. Libaert (2022) illustre

ce dilemme avec l'exemple de la catastrophe de Bhopal, dont le bilan évoluait d'heure en heure dans les premières communications. La littérature résout cette tension par ce que l'on pourrait appeler la communication évolutive : communiquer rapidement sur ce que l'on sait, reconnaître explicitement les limites de l'information disponible, et s'engager à fournir des mises à jour régulières. Cette approche préserve les bénéfices du stealing thunder tout en évitant les risques de la désinformation précipitée.

4.5 Excuses, reconnaissance de responsabilité et action corrective

La question des excuses corporatives dans la gestion des crises est l'une des plus étudiées dans la littérature, avec des résultats nuancés. Chung et Lee (2017) distinguent deux types d'excuses. Les excuses orientées vers la responsabilité (responsibility-oriented apology) reconnaissent explicitement la culpabilité de l'organisation et son obligation de réparation. Les excuses orientées vers la sympathie (sympathy-oriented apology) expriment la compassion et la préoccupation pour les victimes sans nécessairement admettre la culpabilité. Dans une étude expérimentale sur 376 participants, Chung et Lee (2017) montrent que les premières réduisent davantage la colère et la méfiance dans les situations de crises internes et contrôlables — ce qui correspond précisément au cas de nombreuses fuites de données dues à des négligences sécuritaires.

Lee (2004) confirme cette orientation : les stratégies acceptant la responsabilité — excuses directes, compensation, action corrective — sont associées à des scores de confiance plus favorables que les stratégies défensives. Ce résultat est cohérent avec les prescriptions de la SCCT pour les crises à forte attribution de responsabilité.

Benoit (1997) identifie la mortification — reconnaissance complète de la responsabilité assortie d'une demande de pardon — comme la stratégie de réparation la plus directe. Cornelissen (2023) précise que la mortification doit être articulée avec l'action corrective pour être crédible: les mots doivent être suivis d'actes. L'action corrective (rectification) désigne les mesures prises pour remédier aux problèmes — renforcement des systèmes de sécurité, révision des procédures, sanctions internes — et pour prévenir leur récurrence. Sans action corrective visible, les excuses risquent d'être perçues comme purement rhétoriques.

Coombs (2014) met en garde contre le risque particulier du déni suivi d'une révélation de responsabilité. Si l'organisation nie toute responsabilité et qu'il est ensuite établi qu'elle en porte une part, les dommages sont considérablement amplifiés. Frandsen et Johansen (2010)

qualifient ce phénomène de « double crise » : la première crise est l'incident lui-même, la seconde est la révélation de la tentative de dissimulation. Cette double crise est particulièrement dommageable car elle combine les effets de la crise initiale avec une violation de confiance supplémentaire.

Gillespie et Dietz (2009) proposent, dans cette perspective, un processus de réparation de la confiance en quatre étapes séquentielles. La première est la reconnaissance de la violation et de ses impacts sur les parties prenantes : cette étape exige une communication explicite sur ce qui s'est passé, qui a été affecté et comment. La deuxième est l'explication des causes : elle répond au besoin des parties prenantes de comprendre comment l'incident a pu se produire. La troisième est la démonstration de l'engagement à changer : elle signale que l'organisation a tiré les leçons de l'incident et qu'elle est déterminée à ne pas le répéter. La quatrième est l'apport de preuves tangibles de ce changement : elle transforme les engagements en actes vérifiables. Cette séquence — reconnaître, expliquer, agir, prouver — est robuste et convergente avec les prescriptions de la SCCT et de l'Image Repair Theory.

4.6 Stratégies défensives et minimisation : une tentation contre-productive

Les stratégies défensives — minimisation, déni, désignation d'un bouc émissaire — constituent une tentation compréhensible pour les organisations confrontées à une fuite de données. Les équipes juridiques les encouragent souvent, pour limiter l'exposition à des poursuites civiles et pénales. La littérature académique est pourtant quasi unanime sur leur inadéquation dans les crises à forte attribution de responsabilité.

Coombs (2014) formule deux mises en garde explicites. D'une part, le scapegoating (bouc émissaire) génère des réactions négatives : les parties prenantes attendent de l'organisation qu'elle assume la responsabilité ultime de ses produits et services, et non qu'elle tente de se défausser sur un fournisseur ou un sous-traitant. Il cite l'exemple de Mattel, qui a tenté d'attribuer la présence de plomb dans ses jouets à un fournisseur chinois : les clients ont réagi négativement, estimant que Mattel devait assumer la responsabilité finale de ses produits. D'autre part, le déni pur représente un risque majeur si des preuves de responsabilité émergent par la suite.

Cornelissen (2023) illustre les effets d'une communication défensive à travers le cas Boeing et les crashs du 737 Max : « The overall tone of its communication throughout has also been defensive: explaining the technicalities of the software update that may be behind the crashes,

rather than communicating in a more humane and direct manner. » Même dans une crise techniquement complexe, une réponse techniciste et insuffisamment empathique est perçue comme de la minimisation. Ce cas enseigne que dans les crises à fort enjeu humain, les parties prenantes attendent d'abord une réponse émotionnelle et empathique, avant les explications techniques.

Roux-Dufort (2003, cité dans Libaert, 2022) confirme que les stratégies minimalistes créent un écart de perception qui ne joue jamais en faveur de l'organisation : « si des positions claires ne sont pas prises par l'entreprise, d'autres les prendront sans beaucoup d'effort. Si l'information n'est pas donnée alors d'autres formuleront leurs hypothèses et fourniront leurs données. » Ce vide communicationnel est rapidement occupé par des acteurs — journalistes, activistes, lanceurs d'alerte — dont les narratifs sont souvent moins favorables à l'organisation que ce qu'elle aurait pu construire elle-même.

Il existe cependant des situations dans lesquelles les stratégies défensives peuvent être appropriées. Coombs (2007) note que le déni est la stratégie correcte lorsque l'organisation ne porte effectivement aucune responsabilité — notamment dans les cas de rumeurs infondées ou de crises d'origine externe. Dans le contexte des fuites de données causées par une cyberattaque externe, une forme de distanciation modérée peut être légitime, à condition d'être couplée avec des mesures concrètes de remédiation et de protection des victimes.

4.7 Réseaux sociaux et communication digitale de crise

Les réseaux sociaux jouent simultanément le rôle de déclencheurs, d'amplificateurs et de canaux de réponse dans les crises liées aux fuites de données. Cette triple nature fait d'eux un terrain de communication à la fois incontournable et risqué pour les organisations en crise.

Schultz, Utz et Göritz (2011) ont mené une étude expérimentale comparant les effets de la communication de crise via Twitter, les blogs et les médias traditionnels. Leur résultat le plus marquant est que le médium importe davantage que le message : pour les trois variables étudiées — réputation, communication secondaire et réactions comportementales — des effets principaux du médium ont été observés indépendamment du contenu. Ce résultat a des implications stratégiques importantes : le choix des canaux de communication est une décision stratégique à part entière, qui ne peut être laissée au hasard ou à la commodité.

Ki et Nekmat (2014), dans leur analyse des pratiques de communication de crise des entreprises Fortune 500 sur Facebook, montrent que l'engagement actif dans une communication

bidirectionnelle — répondre directement aux commentaires et questions des utilisateurs — est associé à une tonalité significativement plus positive dans les réactions du public. La communication dialogique, qui implique non seulement d'émettre des messages mais aussi de répondre aux questions, d'admettre les incertitudes et d'interagir avec les parties prenantes, est nettement plus efficace que la communication unidirectionnelle.

Catellani (2022) illustre la puissance des réseaux sociaux dans la gestion de crise à travers plusieurs exemples. Elle mentionne le cas de United Airlines, qui a dû présenter des excuses publiques sur Facebook à la suite de deux incidents viraux. Elle cite également le cas de Quick, dont l'ensemble de la communication de crise suite au décès d'un adolescent a été orchestrée sur sa page Facebook, avec des vidéos régulières du directeur général. Dans ce cas, la transparence de la communication sur les réseaux sociaux — y compris les commentaires très critiques auxquels elle n'a pas cherché à répondre de manière défensive — a finalement joué en faveur de l'entreprise.

Cornelissen (2023) analyse la double nature des médias sociaux pour la gestion de crise : un risque — en accélérant la propagation des informations négatives et en permettant aux parties prenantes de s'organiser rapidement — et une opportunité — en offrant des canaux directs, rapides et dialogiques. Il insiste sur la notion de paracrisis (Coombs & Holladay, 2012, cités dans Cornelissen, 2023) : ces signaux d'alerte visibles publiquement — un tweet virulent, une pétition en ligne, un hashtag négatif — qui peuvent dégénérer en crises majeures si on ne les adresse pas rapidement. La surveillance active des réseaux sociaux et une réactivité rapide aux premières alertes sont des composantes essentielles de la préparation à la crise.

Jin, Liu et Austin (2014) mettent en lumière le rôle d'amplificateurs joué par les influenceurs spécialisés en cybersécurité dans les crises de données. Ces acteurs, dotés d'une expertise technique reconnue par leur communauté, peuvent contribuer à établir ou à remettre en cause le cadrage de la crise. Catellani (2022) souligne que les influenceurs sont « des relais d'opinion à traiter avec prudence ». Une organisation qui sait engager proactivement ces acteurs clés de l'écosystème numérique dispose d'un avantage communicationnel significatif.

En synthèse, les fuites de données constituent une forme de crise aux caractéristiques propres : nature numérique, temporalité décalée, effets réputationnels en cascade, multiplicité des audiences et des canaux. La littérature converge vers quatre principes communicationnels fondamentaux : la transparence proactive (stealing thunder), l'acceptation proportionnée de la

responsabilité, l'action corrective démonstrative, et la communication dialogique sur les plateformes numériques.

5. Construction du modèle d'analyse et formulation des hypothèses

Ce cinquième chapitre constitue le passage entre la revue de littérature et la recherche empirique. Il s'agit de transformer les théories et concepts développés dans les chapitres précédents en un outil concret d'analyse, puis de formuler les hypothèses de travail qui guideront notre démarche.

5.1 Justification des choix théoriques

La revue de littérature a permis d'identifier plusieurs cadres théoriques pertinents pour l'analyse des stratégies de communication en situation de fuite de données. Parmi ceux-ci, nous retenons principalement la SCCT (Coombs, 2007) et l'Image Repair Theory (Benoit, 1997) comme théories structurantes, enrichies par les apports de Cornelissen (2023), Gillespie et Dietz (2009), et les travaux empiriques sur les fuites de données (Syed, 2020 ; Martin et al., 2017 ; Goode et al., 2017 ; Schultz et al., 2011 ; Ki & Nekmat, 2014 ; Arpan & Roskos-Ewoldsen, 2005).

La SCCT est retenue comme théorie structurante principale pour plusieurs raisons complémentaires. Elle repose sur des données empiriques solides issues de recherches expérimentales, ce qui lui confère une robustesse supérieure aux approches uniquement fondées sur des études de cas. Elle s'appuie sur un mécanisme psychologique documenté — la théorie de l'attribution — qui permet de modéliser les réactions des parties prenantes de manière prédictive. Elle fournit un cadre prescriptif clair pour chaque type de crise, facilitant l'analyse comparative entre cas. Elle a enfin été explicitement testée dans le contexte des fuites de données par Syed (2020), ce qui valide sa pertinence spécifique pour notre objet d'étude.

L'Image Repair Theory vient compléter ce premier cadre sur la dimension rhétorique et discursive des messages. Là où la SCCT raisonne en termes de stratégie globale, Benoit s'intéresse aux choix d'énonciation — aux mots, aux formulations, aux métaphores mobilisées dans les communications de crise. Cette dimension discursive est essentielle pour analyser la communication des organisations : deux organisations peuvent adopter la même stratégie globale (par exemple, l'acceptation de responsabilité) tout en mobilisant des rhétoriques très différentes. Cornelissen (2023) articule ces deux théories avec la communication corporate, les parties prenantes, l'identité organisationnelle et les médias sociaux, en offrant une perspective

plus englobante. L'ensemble constitue un dispositif théorique robuste, multidimensionnel et empiriquement fondé.

5.2 Le modèle d'analyse : cinq dimensions analytiques

Sur la base des théories retenues, nous proposons un modèle d'analyse structuré autour de cinq dimensions, opérationnalisées en indicateurs empiriquement observables dans les communications des organisations et dans les entretiens qualitatifs conduits auprès de responsables de la communication et de responsables informatiques.

Dimension	Questions d'analyse	Indicateurs empiriques	Ancrage théorique
D1 — Temporalité	La communication a-t-elle été proactive ou réactive ? Dans quel délai ?	Délai détection → divulgation ; conformité RGPD 72h ; stealing thunder ou révélation externe	Coombs (2014) ; Arpan & Roskos-Ewoldsen (2005) ; RGPD art. 33-34
D2 — Stratégie discursive	Quelle stratégie rhétorique domine ? Quel niveau de responsabilité est accepté ?	Type SCCT (deny/diminish/rebuild) ; catégorie Benoit ; nature de l'excuse (responsibility vs sympathy-oriented)	Coombs (2007) ; Benoit (1997) ; Cornelissen (2023) ; Chung & Lee (2017)
D3 — Canal de communication	Quels canaux ont été utilisés ? La communication est-elle dialogique ou unidirectionnelle ?	Canaux mobilisés (communiqué, site web, RS, email, conférence) ; proportion RS vs médias classiques ; engagement dialogique	Schultz et al. (2011) ; Ki & Nekmat (2014) ; Jin et al. (2014)
D4 — Public et registre	À qui s'adresse-t-on en priorité ? Quel registre émotionnel est mobilisé ?	Segmentation des audiences ; registre dominant (empathique, défensif, neutre, technique) ; messages spécifiques aux victimes	Jin et al. (2014) ; Coombs (2007) ; Libaert (2022)
D5 — Action corrective	Quelles mesures correctives ont été annoncées et mises en œuvre ? Sont-elles cohérentes dans le temps ?	Nature et portée des mesures ; formes de compensation ; cohérence discours/actes	Benoit (1997) ; Gillespie & Dietz (2009) ; Goode et al. (2017) ; Cornelissen (2023)

5.3 Formulation des hypothèses de travail

Sur la base de ce modèle, quatre hypothèses de travail guideront notre analyse empirique. Elles couvrent les dimensions temporelle, stratégique, digitale et opérationnelle de la communication de crise, et s'appuient chacune sur des fondements théoriques et empiriques explicites.

Hypothèse 1 (H1) — Transparence et rapidité

Les entreprises qui communiquent proactivement sur la fuite dans les 72 heures suivant sa découverte (stealing thunder) présentent une atteinte réputationnelle moins sévère et une restauration de la confiance plus rapide que celles qui attendent une révélation externe.

Cette hypothèse s'appuie sur Arpan et Roskos-Ewoldsen (2005), qui ont démontré expérimentalement que la divulgation proactive génère des évaluations de crédibilité significativement plus élevées. Coombs (2014) confirme que l'organisation divulgatrice subit moins de dommages réputationnels. Martin et al. (2017) montrent que la transparence sur les pratiques de gestion des données atténue les effets négatifs d'une violation. Les obligations légales du RGPD (articles 33 et 34) constituent un cadre juridique qui s'aligne sur ces prescriptions académiques.

L'hypothèse prédit également que le délai de communication a une incidence sur la sévérité des conséquences réputationnelles : plus l'organisation tarde à communiquer, plus les parties prenantes ont le temps de construire des attributions négatives en l'absence d'information officielle, et plus les rumeurs et les narratifs défavorables ont le temps de se répandre.

Hypothèse 2 (H2) — Adéquation stratégique

Les entreprises adoptant des stratégies accommodatives — full apology, rectification, remediation — en réponse à des fuites impliquant de fortes attributions de responsabilité interne obtiennent de meilleures évaluations réputationnelles post-crise que celles qui privilégient des stratégies défensives (deny, diminish).

Cette hypothèse s'appuie sur le principe central de la SCCT (Coombs, 2007) : les stratégies de communication doivent être proportionnées au niveau de responsabilité attribué. Dans les crises à forte attribution de responsabilité — comme les fuites de données causées par des négligences sécuritaires —, les stratégies accommodatives sont prescrites comme les plus efficaces. Claeys, Cauberghe et Vyncke (2010) ont confirmé expérimentalement que les stratégies de reconstruction conduisent aux meilleures restaurations réputationnelles pour les crises préventables. Chung et Lee (2017) ont montré que les excuses orientées vers la responsabilité réduisent davantage la colère dans les crises internes et contrôlables. Benoit (1997) identifie la mortification comme la stratégie de réparation la plus directe.

Cette hypothèse prédit également la contre-performance des stratégies défensives : le déni ou la minimisation dans un contexte de forte responsabilité organisationnelle devrait être associé

à des scores réputationnels plus dégradés que l'acceptation de responsabilité. Ce résultat serait cohérent avec les mises en garde de Coombs (2014) sur le risque de « double crise ».

Hypothèse 3 (H3) — Communication digitale et dialogique

L'utilisation proactive et dialogique des réseaux sociaux lors de la gestion d'une fuite de données est associée à une perception publique plus favorable et à une moindre diffusion de contenus négatifs.

Cette hypothèse s'appuie sur les résultats de Schultz, Utz et Göritz (2011), qui ont montré que le choix du médium influence les réactions indépendamment du contenu. Ki et Nekmat (2014) ont montré que l'engagement dialogique sur Facebook est associé à une tonalité plus positive dans les réactions du public. Jin, Liu et Austin (2014) ont montré que les publics préfèrent recevoir l'information directement de l'organisation pour les crises d'origine interne. Catellani (2022) souligne l'importance de la cohérence de la communication à travers l'ensemble des plateformes.

Cette hypothèse distingue spécifiquement la communication dialogique — répondre aux questions, engager les conversations, admettre les incertitudes — de la communication unidirectionnelle, en prédisant que la première est plus efficace pour maintenir la confiance des parties prenantes dans un contexte de crise numérique.

Hypothèse 4 (H4) — Action corrective et reconstruction de la confiance

Les entreprises annonçant et mettant en œuvre des actions correctives concrètes, visibles et cohérentes avec leurs engagements — renforcement de la sécurité, compensation des victimes, audits indépendants — reconstituent leur capital de confiance plus efficacement que celles dont la communication se limite à des déclarations symboliques non suivies d'effets.

Cette hypothèse s'appuie sur Benoit (1997), pour qui l'action corrective est une composante essentielle de la réparation de l'image. Gillespie et Dietz (2009) ont montré que la reconstruction de la confiance nécessite des preuves tangibles de changement, et non de simples déclarations d'intention. Goode et al. (2017) ont montré que la compensation calibrée est un levier de restauration de la confiance post-crise. Cornelissen (2023) insiste sur la nécessité d'une cohérence entre les actes et les mots comme fondement de l'authenticité organisationnelle.

Cette hypothèse prédit également que les organisations dont les actions correctives sont documentées, vérifiables et communiquées de manière transparente bénéficient d'une prime de

confiance par rapport à celles dont les engagements restent vagues ou non suivis d'effets. Elle souligne l'importance du suivi post-crise dans la reconstruction réputationnelle à long terme.

5.4 Articulation entre modèle d'analyse, hypothèses et méthodologie

Les quatre hypothèses et le modèle à cinq dimensions seront vérifiés lors de la partie empirique à travers une démarche qualitative en deux volets. Le premier volet consistera en des entretiens semi-directifs conduits auprès de directeurs et responsables de la communication, de responsables informatiques et cybersécurité, et de Managing Directors ou directeurs généraux ayant une expertise en communication de crise. L'objectif est d'accéder aux logiques de décision communicationnelle internes, aux contraintes perçues et aux évaluations rétrospectives des stratégies adoptées.

Le second volet consistera en une analyse des communications officielles produites dans les semaines suivant la révélation de la fuite : communiqués de presse, publications sur les réseaux sociaux, notifications légales, déclarations de dirigeants. La grille à cinq dimensions servira d'outil de codage systématique pour les deux types de matériaux, permettant une analyse comparative rigoureuse entre les cas étudiés.

Les hypothèses seront évaluées à la lumière des résultats obtenus, permettant de confronter les prescriptions théoriques aux pratiques observées. L'objectif final est de dégager des conclusions sur les déterminants d'une communication efficace en situation de fuite de données — des conclusions qui puissent être utiles non seulement à la recherche académique, mais aussi aux praticiens confrontés à ces situations.

En synthèse, ce cinquième chapitre a transformé le cadre théorique en un outil opérationnel. La grille proposée — structurée autour de la temporalité, de la stratégie discursive, du canal, du public et de l'action corrective — offre un cadre de codage rigoureux, ancré dans la SCCT, l'Image Repair Theory et la communication corporate. Les quatre hypothèses de travail formulent des prédictions précises sur les déterminants d'une communication de crise efficace en cas de fuite de données. Elles constituent le fil directeur de la recherche empirique et permettront, à terme, d'évaluer dans quelle mesure les pratiques observées s'alignent sur les prescriptions théoriques.

Q	Thème	Dimensions	Hypothèses	Profils prioritaires
1–2	Profil et contexte	Toutes	—	Tous
3	Fuite comme crise — impacts	D1, D4	**H1, H2**	Tous
4	Expérience vécue	D1, D2, D3, D4, D5	**H1, H2, H3, H4**	Tous
5	Temporalité — stealing thunder	D1	**H1**	Communication, IT
6	Stratégie discursive — excuses	D2, D4	**H2**	Communication, Management
7	Canaux — réseaux sociaux	D3	**H3**	Communication, Management
8	Actions post-crise — confiance	D5	**H4**	Tous
9	Plan de crise — préparation	D1, D5	**H1, H4**	Communication, IT
10	Synthèse — recommandations	Toutes	**H1, H2, H3, H4**	Tous

PARTIE II — RECHERCHE EMPIRIQUE

Le cadre théorique développé dans la première partie de ce mémoire a permis de construire un modèle d'analyse à cinq dimensions — temporalité, stratégie discursive, canal de communication, public et registre, action corrective — ainsi que quatre hypothèses de travail (H1 à H4) portant sur les déterminants d'une communication de crise efficace en situation de fuite de données. Cette seconde partie a pour objectif de confronter ce modèle au terrain. Le chapitre 6 expose la méthodologie retenue pour cette mise à l'épreuve empirique : la posture de recherche adoptée, la constitution du corpus, le déroulement de la collecte et la méthode d'analyse des données. Le chapitre 7 présente ensuite les résultats en deux temps, conformément à la structure demandée : une analyse descriptive, consacrée à la comparaison systématique des cas de communication et des entretiens, puis une analyse interprétative et une discussion théorique, qui reprennent le modèle d'analyse et les hypothèses pour en évaluer la pertinence à la lumière des données recueillies.

6. Méthodologie de la recherche empirique

Ainsi que le rappelle le séminaire d'accompagnement au mémoire, la méthode constitue « le signe distinctif d'une étude scientifique et la pierre angulaire qui la connecte directement aux données du terrain ». Le présent chapitre vise donc à décrire, avec le niveau de détail et de transparence attendu, la manière dont cette recherche a été conduite, en veillant à la cohérence entre la question de recherche — quelle stratégie de communication une entreprise met-elle en place auprès du grand public en cas de fuite de données ? — et les outils mobilisés pour y répondre.

6.1 Posture de recherche

Cette recherche s'inscrit dans une posture compréhensive et interprétative. L'objectif n'est pas de mesurer, sur un large échantillon, la fréquence statistique de telle ou telle pratique communicationnelle, mais de comprendre les logiques de décision, les représentations et les justifications que mobilisent les acteurs — responsables communication, responsables informatiques et cybersécurité, experts en gestion de crise — lorsqu'ils envisagent ou vivent une fuite de données. Cette option se justifie par la nature même de la question de recherche, qui porte sur des perceptions, des arbitrages et des pratiques situées, davantage que sur des grandeurs mesurables.

La démarche suivie n'est ni purement déductive ni purement inductive, mais abductive, faite d'allers-retours entre théorie et terrain — logique que le séminaire décrit comme non linéaire et non mécanique. Le point de départ est déductif : le modèle à cinq dimensions et les quatre hypothèses ont été construits à partir de la littérature (SCCT, Image Repair Theory, communication corporate, littérature spécifique aux fuites de données) avant la collecte. Mais la collecte elle-même a fait émerger des éléments non anticipés par ce cadre — l'existence quasi systématique de deux cellules de crise distinctes, technique et communicationnelle, le poids des réglementations sectorielles telles que DORA au Luxembourg, ou encore le refus assumé des profils informatiques de prendre la parole publiquement — qui sont réintégrés dans l'analyse interprétative (voir 7.2.7). Cette circularité assumée entre théorie et données constitue la garantie d'une recherche à la fois rigoureuse et sensible au terrain.

Nous nous efforçons, conformément aux exigences rappelées par le séminaire, d'être réflexif quant aux limites de sa position — la recherche mobilise des données déclaratives et rétrospectives, recueillies auprès de professionnels qui parlent en partie de leur propre pratique —, rigoureux dans la collecte et l'analyse, et capable de prendre la distance analytique nécessaire vis-à-vis des discours recueillis.

6.2 Un design qualitatif à deux volets complémentaires

Le choix d'une méthode qualitative découle directement de la nature de la question de recherche. Comme le rappelle le séminaire, l'orientation qualitative se prête particulièrement à l'analyse de discours, à l'analyse thématique et à la comparaison sur un nombre restreint de cas — par opposition à l'orientation quantitative, mieux adaptée à l'analyse lexicale ou statistique de corpus volumineux (de l'ordre de plusieurs milliers d'unités). Le volet exploratoire quantitatif mené en amont de ce mémoire (questionnaire diffusé auprès du grand public) a permis de dégager de premières tendances sur les attentes des parties prenantes ; il ne pouvait cependant pas, par construction, rendre compte des logiques de décision internes aux organisations, ni de la construction fine des messages de crise. C'est pour combler cette limite que la partie empirique du mémoire repose sur une démarche qualitative, structurée en deux volets complémentaires et mis en dialogue l'un avec l'autre.

Le premier volet est constitué d'entretiens semi-directifs conduits auprès de professionnels directement concernés par la gestion d'une fuite de données, qu'ils l'aient vécue eux-mêmes ou qu'ils interviennent en amont ou en aval de ce type de crise. Le second volet est un corpus de

cas de communication de crise réellement survenus, analysé à partir des communications officielles disponibles publiquement (communiqués de presse, décisions d'autorités de contrôle, couverture de presse spécialisée). La mise en regard de ces deux volets permet une forme de triangulation méthodologique : les logiques que rapportent les professionnels interrogés peuvent être confrontées aux traces observables des pratiques effectivement mises en œuvre par des organisations tierces, renforçant la validité des constats.

6.3 Constitution du corpus

6.3.1 Volet 1 — les entretiens semi-directifs

Cinq entretiens semi-directifs ont été conduits auprès de professionnels basés au Luxembourg et en Belgique, occupant des fonctions en lien direct avec la sécurité de l'information, la communication corporate ou le conseil en gestion de crise. L'échantillonnage retenu est raisonné et non probabiliste, ce qui est cohérent avec une logique qualitative : il ne s'agit pas de représenter statistiquement une population, mais de constituer un ensemble de points de vue suffisamment contrastés — en matière de fonction, de secteur et de proximité avec une crise vécue — pour permettre une comparaison féconde. Cette diversité recoupe directement les « profils prioritaires » identifiés dans la construction du guide d'entretien (chapitre 5, 5.4) : des profils informatiques et cybersécurité, des profils communication, et un profil d'expertise transversale en gestion de crise.

Conformément aux exigences de confidentialité de la recherche, chaque répondant s'est vu attribuer un pseudonyme. Le poste occupé et le secteur d'activité, en revanche, sont mentionnés, dans la mesure où ils constituent une donnée d'analyse pertinente et ne permettent pas, en tant que tels, d'identifier la personne interrogée.

Pseudonyme	Fonction	Secteur / organisation	Profil
Marc	Chief Information Security Officer (CISO)	Compagnie d'assurance, Luxembourg	IT / cybersécurité
Julien	Deputy Chief Information Officer (DCIO)	Opérateur de télécommunications, Belgique	IT / cybersécurité

Pseudonyme	Fonction	Secteur / organisation	Profil
Sophie	Responsable Marketing et Communication, membre de la direction	Banque, Luxembourg	Communication
Claire	Head of Corporate Communication	Banque, Luxembourg	Communication
Isabelle	CEO, société de conseil en communication stratégique et gestion de crise	Conseil, multi-secteurs, Luxembourg	Expertise transversale

Cet échantillon de cinq personnes présente une double richesse pour l'analyse : d'une part, il permet de comparer les logiques propres aux fonctions techniques (Marc, Julien) à celles des fonctions communication (Sophie, Claire), qui n'abordent pas la crise avec les mêmes priorités ni le même vocabulaire ; d'autre part, le témoignage d'Isabelle, gestionnaire de crise transversale intervenant auprès de multiples organisations, offre un point de vue comparatif à lui seul, puisqu'il synthétise des observations issues de plusieurs terrains.

6.3.2 Volet 2 — un corpus de cas de communication de crise

N'ayant pas eu accès aux échanges internes des organisations tierces ayant traversé une fuite de données, ce second volet s'appuie sur les traces publiques de leur communication de crise : communiqués de presse officiels, décisions et communiqués des autorités de protection des données (CNIL en France, CNPD au Luxembourg), ainsi que couverture de presse spécialisée en cybersécurité et en droit du numérique. Cette source documentaire, bien que ne donnant pas accès aux délibérations internes, permet néanmoins d'observer les manifestations concrètes des cinq dimensions du modèle d'analyse : ce qui a été dit, quand, par quel canal, à quel public et avec quelles suites opérationnelles.

Trois critères ont guidé la sélection des cas : la diversité sectorielle et de résultats (l'échantillon devait inclure des issues contrastées, et non uniquement des cas de réussite, afin d'éviter l'écueil dénoncé par le séminaire consistant à collecter uniquement les données confirmant la thèse recherchée) ; la récence, l'ensemble des cas retenus se situant en 2024, dans un cadre

réglementaire européen homogène (RGPD) ; et la disponibilité d'une documentation suffisamment étoffée pour permettre un codage selon la grille à cinq dimensions. Quatre cas ont ainsi été retenus.

Cas	Secteur	Origine des données
Boulanger	Distribution (électroménager / multimédia), France	Communiqué client, presse spécialisée (Usine Digitale, Le Monde Informatique, INCYBER)
France Travail (ex-Pôle emploi) et Cap emploi	Service public de l'emploi, France	Communiqué officiel, communiqué et décision de sanction de la CNIL, presse spécialisée
Free et Free Mobile	Télécommunications, France	Décision de sanction de la CNIL (SAN-2026-001 et 002), presse spécialisée et associative
Opérateur télécoms (cas relaté par Julien)	Télécommunications, Belgique / groupe international	Entretien semi-directif (volet 1) — perspective interne, non recoupée par une analyse documentaire indépendante

Le quatrième cas mérite une remarque méthodologique particulière : il ne provient pas d'une recherche documentaire indépendante, mais du récit qu'en fait Julien lui-même au cours de son entretien. Il est donc traité, dans l'analyse descriptive, au même titre que les trois autres cas — en tant que matériau du volet « textes » — mais sa nature de témoignage interne, potentiellement empreint de justification a posteriori, appelle une prudence interprétative particulière, discutée en 6.7 et en 7.1.1.

6.4 Élaboration du guide d'entretien

Le guide d'entretien a été construit directement à partir du modèle d'analyse à cinq dimensions et des quatre hypothèses de travail présentés au chapitre 5 (tableau 5.2, 5.3 et 5.4), de manière à garantir la cohérence entre cadre théorique et collecte de terrain. Il comporte dix questions ouvertes, organisées en deux blocs. Le premier bloc (questions 1 et 2) porte sur le profil et le

contexte professionnel du répondant. Le second bloc (questions 3 à 10) aborde successivement la perception de la fuite de données comme crise spécifique, l'expérience vécue le cas échéant, la temporalité de la communication et le principe du stealing thunder, la stratégie discursive et la question des excuses, les canaux et notamment les réseaux sociaux, les actions post-crise et la reconstruction de la confiance, l'existence d'un plan de crise formalisé, et enfin une synthèse sous forme de recommandations.

Chaque question du guide a été rattachée, dès sa conception, à une ou plusieurs dimensions du modèle d'analyse et, le cas échéant, à une ou plusieurs hypothèses, ce qui a permis un codage direct des réponses lors de l'analyse (voir 6.6). Le format semi-directif a été privilégié afin de conserver la souplesse nécessaire à l'expression spontanée des répondants, tout en assurant une couverture systématique des thèmes centraux pour l'analyse comparative. L'ordre et la formulation exacte des questions ont pu être légèrement adaptés selon le profil de l'interlocuteur — un responsable informatique et un responsable communication n'étant pas interrogés dans les mêmes termes sur, par exemple, le contenu et le ton des messages.

6.5 Déroulement de la collecte

Les cinq entretiens ont été conduits individuellement, en français, avec l'accord préalable des personnes interrogées quant à l'enregistrement et à l'utilisation des propos dans le cadre de ce mémoire. Chaque entretien a fait l'objet d'un enregistrement intégral puis d'une retranscription verbatim, consignée dans un document dédié. Cette retranscription constitue la matière première de l'ensemble des analyses présentées au chapitre 7 : toute citation ou paraphrase mobilisée dans ce qui suit y renvoie directement.

Conformément à l'engagement de confidentialité pris envers les répondants, l'identité de chacun a été anonymisée dans l'ensemble du mémoire au moyen d'un pseudonyme (voir tableau 6.1). Cette anonymisation porte sur l'identité des personnes ; la fonction occupée et le secteur d'activité sont en revanche conservés, dans la mesure où ils constituent une variable d'analyse et ne permettent pas, à eux seuls, une identification univoque des répondants.

6.6 Méthode d'analyse des données

L'analyse des données recueillies — entretiens et cas de communication — a été conduite selon une démarche d'analyse de contenu thématique, appuyée sur un codage manuel structuré par la grille à cinq dimensions (D1 Temporalité, D2 Stratégie discursive, D3 Canal de

communication, D4 Public et registre, D5 Action corrective) élaborée au chapitre 5. Cette grille fonctionne comme un outil de codage déductif commun aux deux volets du corpus, ce qui garantit la comparabilité entre les cas de communication et les entretiens. Elle a été complétée, en cours d'analyse, par des catégories émergentes non anticipées par le cadre théorique initial — telles que l'existence de cellules de crise distinctes (technique et communication), le poids de réglementations sectorielles (DORA, CSSF) ou la segmentation des publics entre clientèle grand public et grands comptes —, discutées en 7.2.7.

L'analyse s'est déroulée en deux temps distincts, correspondant aux deux sections du chapitre 7. Une analyse descriptive a d'abord été menée, consistant à comparer systématiquement, dimension par dimension et thème par thème, d'une part les quatre cas de communication entre eux, d'autre part les cinq entretiens entre eux, sans chercher à ce stade à interpréter ces constats à la lumière de la théorie. Cette étape descriptive vise à établir, de façon aussi neutre que possible, ce qui converge et ce qui diverge dans le corpus. Une analyse interprétative a ensuite été conduite, reprenant le modèle d'analyse et les quatre hypothèses de travail pour confronter les résultats descriptifs aux théories mobilisées dans le cadre théorique (SCCT, Image Repair Theory, stealing thunder, communication corporate, trust repair).

Conformément aux préconisations méthodologiques reçues, aucune donnée n'est présentée sous forme de pourcentage : l'échantillon de cinq entretiens ne s'y prête pas et un tel usage donnerait une fausse impression de représentativité statistique. Les convergences et divergences entre répondants sont en revanche systématiquement quantifiées sous la forme « x répondants sur 5 », ce qui permet de rendre visible le poids relatif d'un constat au sein du corpus sans lui prêter une portée généralisable. Lorsque les cinq répondants convergent, cela est signalé comme un constat unanime du corpus ; lorsque le partage suit une ligne de clivage entre profils (par exemple entre les deux répondants informatiques et les deux répondants communication), cela est également explicité, car cette ligne de clivage constitue en elle-même un résultat d'analyse.

Une attention particulière a été portée à la triangulation, considérée par le séminaire comme un gage de rigueur scientifique : lorsque cela était possible, les propos d'un répondant ont été mis en regard des éléments observables dans le volet documentaire. C'est notamment le cas pour le témoignage de Julien, dont le récit recoupe, dans ses grandes lignes, une fuite de données réellement survenue et documentée dans la presse spécialisée en 2024 au sein du secteur des télécommunications belge, ce qui permet de nuancer son témoignage — par nature auto-rapporté et potentiellement valorisant — par des éléments de contexte externes.

6.7 Posture réflexive et limites méthodologiques

Conformément à l'exigence de réflexivité rappelée par le séminaire, plusieurs limites doivent être explicitées. Premièrement, l'échantillon de cinq entretiens ne permet aucune généralisation statistique ; il donne accès à des logiques d'acteurs et à des lignes de tension entre profils, non à une mesure de leur fréquence dans la population des professionnels concernés. Deuxièmement, l'échantillon présente un biais sectoriel et géographique : quatre répondants sur cinq exercent au Luxembourg, place financière fortement régulée, et une majorité de répondants proviennent de secteurs eux-mêmes très encadrés (banque, assurance) ; les constats relatifs au poids de la réglementation doivent donc être lus avec cette spécificité à l'esprit et ne sont pas nécessairement transférables à des secteurs moins régulés.

Troisièmement, les propos recueillis en entretien sont déclaratifs et rétrospectifs : les répondants décrivent leurs pratiques, ou celles de leur organisation, avec le recul et, potentiellement, un biais de désirabilité sociale — une tendance à présenter sous un jour favorable des pratiques qu'ils ont eux-mêmes contribué à concevoir. Ce biais est particulièrement à surveiller pour le récit de Julien, seul répondant à décrire une crise directement vécue et gérée par son organisation, et dont l'évaluation de l'impact réputationnel externe comme « finalement limité » relève d'une appréciation interne, non validée de façon indépendante dans le cadre de ce mémoire.

Quatrièmement, les trois cas de communication issus de sources documentaires (Boulanger, France Travail, Free) ne donnent accès qu'à ce qui a été rendu public ou établi par une autorité de contrôle ; les délibérations internes qui ont présidé à ces choix de communication demeurent hors de portée de cette recherche. Cinquièmement, cette recherche documente les logiques organisationnelles de production de la communication de crise, mais n'interroge pas directement — dans ce volet — la réception effective de ces messages par leurs publics ; cette dimension réceptive n'est abordée que partiellement, à travers le questionnaire exploratoire mentionné dans le projet de mémoire initial et à travers les représentations qu'en ont les professionnels interrogés.

Enfin, conformément au principe de fidélité aux sources rappelé par le séminaire — selon lequel ce sont les hypothèses qui doivent, le cas échéant, être révisées, et jamais les données —, l'ensemble des constats présentés au chapitre 7 est strictement ancré dans les propos retranscrits et les faits documentés, la grille d'analyse et le guide d'entretien utilisés garantissant par ailleurs la transparence et la possible reproductibilité de la démarche.

7. Analyse et résultats

Ce chapitre présente les résultats de la recherche empirique en deux temps, conformément à la structure retenue. La section 7.1 propose une analyse descriptive : elle compare systématiquement, d'une part les quatre cas de communication de crise constitutifs du volet documentaire, d'autre part les cinq entretiens semi-directifs, en établissant les convergences et les divergences observables dans le corpus, sans encore les interpréter à la lumière de la théorie. La section 7.2 propose une analyse interprétative et une discussion théorique : elle reprend le modèle d'analyse à cinq dimensions et les quatre hypothèses de travail formulés au chapitre 5, pour confronter les constats descriptifs aux cadres théoriques mobilisés — la SCCT, l'Image Repair Theory, le principe du stealing thunder, la communication corporate et la littérature sur la reconstruction de la confiance.

7.1 Analyse descriptive

7.1.1 Comparaison des cas de communication de crise

Les quatre cas retenus — Boulanger, France Travail et Cap emploi, Free et Free Mobile, ainsi que le cas de l'opérateur télécoms relaté par Julien — sont ici comparés selon les cinq dimensions du modèle d'analyse. Le tableau suivant en propose une synthèse ; les développements qui suivent en détaillent les principaux constats.

Dimension	Boulanger	France Travail / Cap emploi	Free / Free Mobile	Opérateur télécoms (cas Julien)
D1 — Temporalité	Attaque dans la nuit du 6 au 7 septembre 2024 ; communication aux clients le 9 septembre, environ 48h après les faits. Communication	Intrusion entre le 6 février et le 5 mars 2024 ; détection tardive (plusieurs semaines) ; notification à la CNIL le 8 mars ; communiqué public le 13 mars, soit près d'une semaine après la détection.	Intrusion entre le 28 septembre et le 22 octobre 2024, soit près d'un mois d'accès non détecté ; notification	Selon le répondant : mise à l'arrêt du système compromis dès les premières heures ; communicatio

Dimension	Boulanger	France Travail / Cap emploi	Free / Free Mobile	Opérateur télécoms (cas Julien)
	partiellement devancée par la divulgation, sur un forum de piratage, d'un volume de données bien supérieur à celui reconnu par l'entreprise.		des abonnés dans un second temps, mais jugée tardive et incomplète par la CNIL au regard de l'article 34 du RGPD.	n publique volontairement différée de quelques jours afin de disposer d'une information stabilisée et de communiquer « en une fois » plutôt qu'en plusieurs vagues.
D2 — Stratégie discursive	Reconnaissance minimale des faits (« acte de cybermalveillance »), portée de la fuite fortement minimisée (adresses de livraison uniquement) et contestée par des chercheurs en sécurité ; aucune formulation d'excuse ; refus de commentaires	Communication factuelle et conforme aux obligations légales, énumération précise des données concernées et non concernées ; registre informatif plutôt qu'accommodant ; lors de la sanction de la CNIL en 2026, reconnaissance de « la gravité des faits » tout en regrettant la sévérité de la sanction — discours mixte entre acceptation et défense.	Notification structurée à deux niveaux (courriel puis numéro vert / DPO) traduisant une intention de transparence, mais jugée insuffisante par la CNIL, qui relève que le message ne permettait pas aux personnes	Triptyque revendiqué par le répondant : « transparent, complet, rapide ». Absence explicite de formulation d'excuse dans le récit, mais reconnaissance implicite de responsabilité à travers l'investisseme

Dimension	Boulanger	France Travail / Cap emploi	Free / Free Mobile	Opérateur télécoms (cas Julien)
	supplémentaires à la presse.		concernées de comprendre pleinement les conséquences ni les mesures de protection à adopter.	nt correctif annoncé.
D3 — Canal	Courriel individuel aux clients concernés ; pas de conférence de presse ; communication essentiellement unilatérale et peu dialogique.	Communiqué de presse officiel, notification individuelle réglementaire, renvoi vers les ressources de la CNIL et de cybermalveillance.gouv.fr ; peu d'éléments observables de communication dialogique sur les réseaux sociaux.	Communication individualisée (courriel, numéro vert) orientée B2C ; peu de communication publique proactive au-delà de l'information réglementaire.	Approche multicanale et segmentée selon le répondant : communiqué de presse officiel, contacts informels avec des journalistes de confiance en amont de la publication, et surtout rencontres individuelles des dirigeants avec les grands comptes

Dimension	Boulanger	France Travail / Cap emploi	Free / Free Mobile	Opérateur télécoms (cas Julien)
				institutionnels sur plusieurs mois — une granularité de canal absente des trois autres cas, purement B2C.
D4 — Public et registre	Registre rassurant et technique, faible empathie apparente, absence de distinction entre profils de clients touchés.	Registre légal et pédagogique, orienté vers la protection individuelle (conseils anti-hameçonnage), s'adressant à un public très large (43 millions de personnes potentiellement concernées) de façon standardisée.	Registre individualisé mais jugé insuffisamment clair par le régulateur ; public très large (19 à 24 millions d'abonnés) incluant des données sensibles (IBAN).	Selon le répondant, distinction marquée entre marché résidentiel (traitement standardisé, faible portée dans le temps) et marché entreprise (traitement individualisé et prolongé, avec rencontres personnalisées des grands clients).

Dimension	Boulanger	France Travail / Cap emploi	Free / Free Mobile	Opérateur télécoms (cas Julien)
D5 — Action corrective	« Vigilance renforcée » évoquée en termes généraux, sans détail public des mesures concrètes engagées.	Généralisation de la double authentification annoncée comme mesure corrective, mais jugée tardive par la CNIL, qui a prononcé une sanction de 5 millions d'euros pour défaut de sécurisation antérieur.	Investissements en sécurité engagés après la crise, mais jugés très insuffisants au regard des manquements constatés ; sanction record de 42 millions d'euros cumulés.	Réorganisation interne substantielle décrite par le répondant : fusion d'équipes de sécurité auparavant séparées, budget dédié à des projets structurels de moyen et long terme, arrêt immédiat du système compromis.

La comparaison de ces quatre cas fait apparaître une convergence et plusieurs divergences significatives. La convergence porte sur le fait que les quatre organisations ont, sans exception, communiqué à leurs publics concernés dans un délai proche de l'obligation réglementaire des 72 heures ou de quelques jours supplémentaires — aucune n'a choisi le silence total, ce qui suggère que la norme de la notification rapide s'est largement imposée dans la pratique, au moins sous sa forme minimale et légale.

Les divergences, en revanche, sont nombreuses et instructives. Sur la dimension D1, seul le cas relaté par Julien illustre une véritable logique de stealing thunder maîtrisée — communication différée volontairement de quelques jours mais contrôlée par l'organisation elle-même — tandis que les trois autres cas montrent des formes de dépossession partielle de l'initiative

informationnelle : chez Boulanger, un tiers (chercheur en sécurité) révèle une ampleur de fuite supérieure à celle reconnue par l'entreprise ; chez France Travail, la lenteur de détection (plusieurs semaines) prive de facto l'organisation de la possibilité d'une divulgation véritablement proactive ; chez Free, la notification, bien que réalisée, est jugée a posteriori incomplète par le régulateur. Sur la dimension D2, les quatre cas évitent tous l'excuse explicite, mais se distinguent par le degré de reconnaissance de la portée réelle de l'incident, allant de la minimisation contestée (Boulanger) à la reconnaissance structurée mais jugée insuffisante (Free), en passant par un registre mixte entre acceptation et défense (France Travail). Sur la dimension D3, seul le cas relaté par Julien présente une segmentation fine des canaux selon les publics (grand public / grands comptes / presse), les trois autres cas se limitant à des canaux unilatéraux standardisés adressés à l'ensemble des personnes concernées. Sur la dimension D5, enfin, les trois cas documentés de façon indépendante (Boulanger, France Travail, Free) montrent tous un décalage, révélé a posteriori par un tiers (chercheur, régulateur), entre les mesures correctives communiquées et les mesures correctives jugées suffisantes, alors que le cas rapporté par Julien ne fait état d'aucune sanction ou contestation externe — étant toutefois rappelé, comme indiqué au chapitre 6, que ce dernier constat repose sur une source unique et auto-rapportée.

7.1.2 Comparaison des entretiens

Les cinq entretiens sont ici comparés systématiquement, thème par thème, en suivant la structure du guide d'entretien (chapitre 6, 6.4). Le tableau suivant synthétise, pour chaque thème central, la position de chacun des cinq répondants.

Thème (question du guide)	**Marc (CISO, assurance)**	**Julien (DCIO, télécoms)**	**Sophie (Marketing/Com, banque)**	**Claire (Corporate Com, banque)**	**Isabelle (conseil, gestion de crise)**
Fuite comme crise — enjeux principaux (Q3)	Triade confidentialité / intégrité / disponibilité ; impact	Impact sur la confiance des grands comptes institutionnels ; distinction	Confiance immédiate, retraits, départs vers la concurrence ;	Confiance ; sensibilité de la donnée (client vs employé) et ampleur	Confiance en premier lieu ; situations paradoxales (accès croisés aux comptes)

Thème (question du guide)	Marc (CISO, assurance)	Julien (DCIO, télécoms)	Sophie (Marketing/Com, banque)	Claire (Corporate Com, banque)	Isabelle (conseil, gestion de crise)
	réputationnel et business.	résidentiel / entreprise.	effet boule de neige.	comme facteurs déterminants.	particulièrement corrosives.
Temporalité — stealing thunder (Q5)	Non directement abordé (pas de crise externe vécue) ; accent mis sur la détection et la préparation.	Ne pas attendre ; obligation légale ; mais éviter les communications fragmentées, préférer une communication complète en une fois.	Prendre la parole rapidement, rassurer, sans trop s'avancer sur ce qui n'est pas encore certain ; la non-communication est la pire des stratégies.	Le plus rapidement possible dès qu'un niveau d'information suffisant est atteint ; risque symétrique à éviter entre parler trop tôt et trop tard.	Délai de 72h jugé tantôt trop long, tantôt trop court selon la gravité et la criticité de l'organisation ; certains secteurs tenus à un délai de 2h envers les autorités.
Ton et stratégie discursive — excuses (Q6)	Non concerné directement (rôle non porte-parole).	Triptyque « transparent, complet, rapide » ; pas de mention explicite d'excuse.	Éviter l'excuse explicite (« on est vraiment désolé ») perçue comme un aveu de perte de contrôle ; assumer sans s'avilir ; rester digne.	Assumer, reconnaître les faits, sans excès d'excuse ; langage simple, sans jargon ; éviter la spéculation.	Ton authentique, fidèle à la culture de l'entreprise ; rejet des formulations génériques produites par l'IA ; empathie

Thème (question du guide)	Marc (CISO, assurance)	Julien (DCIO, télécoms)	Sophie (Marketing/Com, banque)	Claire (Corporate Com, banque)	Isabelle (conseil, gestion de crise)
					envers les victimes et les collaborateurs.
Canaux et réseaux sociaux (Q7)	Non directement abordé (communication externe hors de son périmètre).	Communiqué de presse officiel + relations presse informelles construites en amont + rencontres individuelles des grands comptes.	Choix du canal dépendant de l'audience ; réseaux sociaux jugés propices au négatif mais utiles pour une réassurance rapide et ciblée.	Cercle privé vers l'extérieur (interne puis clients puis presse) ; réseaux sociaux perçus comme une opportunité s'ils sont bien utilisés ; ajout des notifications push comme canal complémentaire.	Pas de canal supérieur en soi ; primauté de l'authenticité et de la cohérence avec les habitudes de communication de l'organisation.
Actions correctives et	Approche structurée de type ISO 27001,	Réorganisation interne, fusion d'équipes,	Outil de veille (détection de sites frauduleux)	Plans de crise testés régulièrement sous	Prudence quant à la communication de

Thème (question du guide)	Marc (CISO, assurance)	Julien (DCIO, télécoms)	Sophie (Marketing/Com, banque)	Claire (Corporate Com, banque)	Isabelle (conseil, gestion de crise)
confiance (Q8)	pilotée par le risque réel.	budget dédié à des projets structurels.	mis en place après incident sectoriel ; investissements attendus en hausse continue.	obligation réglementaire (DORA) ; anticipation plutôt que réaction.	mesures qui auraient dû exister avant la crise (risque d'aveu de négligence) ; confiance reconstruite par des actions concrètes et incrémentales, non par un grand plan de communication.
Plan de crise et préparation (Q9)	Plan de crise obligatoire (ISO 27001, DORA) ; simulations annuelles avec scénarios variés.	Deux cellules indépendantes (technique et communication) coiffées par un responsable commun, identifiées comme la	Cellule de crise opérationnelle testée régulièrement ; arbre décisionnel formalisé précisant qui alerte qui, comment, et avec quel ton.	Plan de crise intégré au dispositif réglementaire européen (tests de résilience) ; groupe d'astreinte mobilisable en urgence.	Triptyque préparation / action / reconstruction ; plan de communication de crise devant être cohérent avec le plan de continuité

Thème (question du guide)	Marc (CISO, assurance)	Julien (DCIO, télécoms)	Sophie (Marketing/Com, banque)	Claire (Corporate Com, banque)	Isabelle (conseil, gestion de crise)
		leçon la plus importante tirée de la crise vécue.			d'activité et révisé au moins deux fois par an.

Cette comparaison fait apparaître un nombre significatif de convergences fortes. Sur la question de la temporalité, quatre répondants sur cinq (Julien, Sophie, Claire, Isabelle) affirment explicitement qu'il ne faut pas attendre pour communiquer et que le silence constitue la pire des stratégies ; Marc, seul, n'aborde pas frontalement cette question, faute d'avoir eu à communiquer publiquement, mais souligne néanmoins l'importance de la détection rapide, ce qui va dans le même sens. Sur l'existence d'un plan de crise formalisé et régulièrement testé, les cinq répondants convergent sans exception — il s'agit du constat le plus unanime du corpus d'entretiens. Sur l'importance d'une action corrective concrète, tangible et incrémentale, plutôt que d'une communication purement déclarative, les cinq répondants convergent également, chacun avec un exemple issu de sa pratique.

Une convergence plus fine, et particulièrement intéressante pour l'analyse interprétative, concerne le rapport à l'excuse : trois répondants sur cinq (Sophie, Claire, Isabelle) abordent explicitement cette question et convergent vers un même refus de l'excuse émotionnelle ou spectaculaire, tout en insistant, dans le même mouvement, sur la nécessité d'assumer les faits et de reconnaître ce qui n'a pas fonctionné. Cette nuance — assumer sans s'excuser au sens fort du terme — constitue une position partagée par l'ensemble des répondants « communication » du corpus, alors même qu'elle n'était pas anticipée sous cette forme précise dans le guide d'entretien.

Les divergences les plus nettes suivent la ligne de partage entre profils informatiques et profils communication. Marc et Julien, les deux répondants issus de fonctions informatiques et cybersécurité, écartent tous deux explicitement l'idée de prendre eux-mêmes la parole publique — Marc l'exprime avec la plus grande netteté (« je n'irai certainement pas répondre à la presse

[…] ce n'est pas mon rôle ») — et centrent leur discours sur des cadres de gestion des risques techniques (triade confidentialité-intégrité-disponibilité pour Marc, réorganisation structurelle pour Julien). Sophie et Claire, les deux répondantes issues de fonctions communication, centrent au contraire leur discours sur la psychologie du public (panique, réassurance, registre) et sur la construction fine du message. Une autre ligne de divergence, plus contextuelle, oppose le cas de Julien — seul répondant ayant vécu une crise majeure directement, dans un contexte B2B fortement institutionnel avec des grands comptes internationaux — aux quatre autres répondants, dont le discours reste largement de l'ordre de la préparation et de l'anticipation plutôt que du retour d'expérience direct sur une communication publique effective.

Enfin, une divergence contextuelle plus large, déjà relevée au chapitre 6, tient au poids de la réglementation sectorielle : les quatre répondants luxembourgeois évoquent spontanément et à plusieurs reprises des cadres tels que DORA, la CSSF ou la CNPD, quand Julien, seul répondant belge et issu d'un secteur non financier, ne les mentionne pas et raisonne davantage en matière de criticité d'infrastructure nationale et de relation avec des points de contact étatiques dédiés. Ce constat, de nature davantage contextuelle que théorique, est repris dans la discussion des apports non anticipés par le cadre théorique initial (7.2.7).

7.2 Analyse interprétative et discussion théorique

Cette section reprend le modèle d'analyse à cinq dimensions et les quatre hypothèses de travail formulés au chapitre 5 (5.2 et 5.3), pour confronter les constats descriptifs établis en 7.1 aux cadres théoriques mobilisés dans la revue de littérature — la SCCT (Coombs, 2007), l'Image Repair Theory (Benoit, 1997), le principe du stealing thunder (Arpan & Roskos-Ewoldsen, 2005 ; Coombs, 2014), la littérature sur la communication digitale de crise (Schultz, Utz & Göritz, 2011 ; Ki & Nekmat, 2014) et sur la reconstruction de la confiance (Gillespie & Dietz, 2009). L'analyse est ici interprétative au sens où elle vise, selon la distinction rappelée par le séminaire, à « tirer une nouvelle information de l'analyse » et à confronter les résultats du terrain à l'arrière-plan théorique, plutôt qu'à simplement les décrire.

7.2.1 H1 — Transparence et rapidité (dimension D1)

Rappel de l'hypothèse. H1 postule que les entreprises communiquant proactivement dans les 72 heures suivant la découverte d'une fuite (stealing thunder) subissent une atteinte réputationnelle moins sévère et restaurent la confiance plus rapidement que celles attendant une révélation externe.

Le corpus corrobore qualitativement l'orientation générale de cette hypothèse : la quasi-unanimité des répondants (quatre sur cinq explicitement, le cinquième par déduction) et l'ensemble des quatre cas documentés convergent vers l'idée qu'une communication rapide est préférable au silence, ce qui rejoint directement Coombs (2014) et la logique du stealing thunder. Mais la mise en regard fine des cas et des entretiens révèle une limite importante, non explicitée dans la formulation initiale de H1 : la proactivité de la divulgation suppose, comme précondition, une capacité de détection rapide de l'incident. Or le cas France Travail montre qu'une détection tardive — l'intrusion serait restée active plusieurs semaines avant d'être repérée — prive mécaniquement l'organisation de la possibilité même d'une divulgation proactive au sens de Coombs, quelle que soit la volonté de transparence affichée ensuite. Le cas Boulanger illustre une seconde limite : la proactivité de l'organisation peut être court-circuitée par la divulgation d'un tiers non maîtrisé — ici, un chercheur en sécurité révélant une ampleur de fuite bien supérieure à celle initialement reconnue —, ce qui remet en question l'idée, implicite dans la littérature du stealing thunder, que l'organisation contrôle nécessairement le récit initial de la crise.

Le témoignage de Julien apporte un raffinement supplémentaire, qui recoupe directement Coombs (2014) tout en le nuançant : la préférence exprimée pour une communication « en une fois » plutôt qu'en plusieurs vagues successives, motivée par le souci d'éviter la confusion, introduit un arbitrage entre rapidité et complétude qui n'est pas résolu de façon univoque par la seule règle des 72 heures. Ce constat rejoint la nuance apportée par Isabelle, qui relativise explicitement le caractère absolu du délai réglementaire : « 72 heures, c'est parfois très long — et parfois très court […] ça dépend vraiment de la gravité de la crise et du rôle de l'organisation dans le fonctionnement de la société », rappelant au passage que certaines infrastructures critiques peuvent être tenues à des délais bien plus courts (deux heures) envers les autorités, dans le cadre de stratégies nationales de résilience distinctes du RGPD.

Statut de l'hypothèse. H1 est partiellement confirmée. La direction de l'effet postulée par la littérature — transparence proactive associée à une gestion de crise plus maîtrisée — est corroborée par l'ensemble du corpus. En revanche, l'opérationnalisation de cette proactivité par un seuil fixe de 72 heures apparaît, au regard du terrain, insuffisante : elle devrait être complétée par deux préconditions non explicitées dans le modèle initial — une capacité de détection rapide de l'incident, sans laquelle la proactivité est structurellement impossible, et une appréciation contextuelle du délai réellement praticable selon la criticité sectorielle de l'organisation, qui peut être inférieure ou légèrement supérieure au seuil réglementaire générique.

7.2.2 H2 — Adéquation stratégique : stratégies discursives et reconnaissance de responsabilité (dimension D2)

Rappel de l'hypothèse. H2 postule que les entreprises adoptant des stratégies accommodatives (excuses complètes, rectification, remédiation) en réponse à des fuites impliquant une forte attribution de responsabilité interne obtiennent de meilleures évaluations réputationnelles que celles privilégiant des stratégies défensives.

La confrontation du corpus à la SCCT (Coombs, 2007) et à l'Image Repair Theory (Benoit, 1997) fait apparaître un résultat à la fois confirmatif et nuancé. Sur le plan des cas documentés, le classement en termes de sévérité de sanction (Boulanger : minimisation contestée, sans sanction publique connue à ce jour ; France Travail : reconnaissance factuelle mais sanction de 5 millions d'euros pour défaut de sécurisation antérieur ; Free : notification structurée mais jugée insuffisante, sanction cumulée de 42 millions d'euros) suggère que la reconnaissance des faits, à elle seule, ne suffit pas à limiter les conséquences si elle n'est pas adossée à une action corrective jugée à la hauteur — ce qui relie directement D2 à D5 et sera repris en 7.2.5. Ce constat rejoint la mise en garde de Cornelissen (2023), pour qui le cadrage des faits vise à influencer l'attribution de responsabilité mais peut se retourner contre l'organisation lorsque ce cadrage est contesté par des acteurs tiers disposant d'une information concurrente — configuration précisément observée dans le cas Boulanger.

Le résultat le plus riche de cette section concerne cependant la forme que prend, dans le discours des professionnels interrogés, l'accommodation prônée par la SCCT et l'Image Repair Theory. Trois répondants sur cinq (Sophie, Claire, Isabelle) abordent explicitement la question de l'excuse et convergent, indépendamment les uns des autres, vers un même refus de la formulation d'excuse au sens classique du terme — Sophie va jusqu'à recommander d'éviter des formulations telles que « c'est catastrophique, on est vraiment désolé », qu'elle juge porteuses d'une impression de perte de contrôle. Or ce même trio recommande, dans le même mouvement, d'assumer les faits, de reconnaître ce qui n'a pas fonctionné et de rester transparent. Cette position ne correspond pleinement ni à une stratégie purement défensive (deny, diminish) au sens de Coombs, ni à la catégorie de la « mortification » au sens de Benoit, qui suppose une forme d'aveu et de contrition explicite. Elle s'apparente davantage à ce que l'on pourrait qualifier de reconnaissance de responsabilité sans confession émotionnelle — une transparence factuelle et digne, qui accepte la responsabilité des faits sans mobiliser le registre affectif de l'excuse.

Cette observation trouve un écho direct dans la distinction proposée par Chung et Lee (2017) entre excuse orientée responsabilité (responsibility-oriented) et excuse orientée sympathie (sympathy-oriented) : le corpus recueilli ici penche nettement vers le premier registre — assumer, nommer les manquements, s'engager sur des actions correctives — plutôt que vers le second, ce qui est cohérent avec le résultat de Chung et Lee selon lequel c'est l'acceptation de responsabilité, davantage que l'expression affective de regret, qui contribue à la restauration de la confiance. Le témoignage d'Isabelle vient renforcer cette lecture en insistant sur l'authenticité du ton — « fidèle à la culture de l'entreprise » — et en mettant en garde contre les formulations génériques produites par l'intelligence artificielle, jugées « lisses » et déshumanisées : l'accommodation recherchée par les praticiens n'est donc pas l'absence de tonalité humaine, mais le refus d'une tonalité spectaculaire ou artificiellement dramatisée.

Statut de l'hypothèse. H2 est confirmée sur le principe général — l'accommodation et la reconnaissance de responsabilité sont associées, dans le corpus, à une gestion de crise jugée plus efficace que la minimisation pure. Elle est toutefois nuancée quant à la forme empirique que prend cette accommodation : celle-ci se manifeste, chez les praticiens interrogés, comme une reconnaissance factuelle et digne de responsabilité plutôt que comme une excuse au sens plein du terme mobilisé par Benoit, ce qui invite à préciser, pour ce contexte sectoriel au moins, la catégorie d'accommodation retenue dans le modèle d'analyse.

7.2.3 H3 — Communication digitale et dialogique (dimension D3)

Rappel de l'hypothèse. H3 postule que l'utilisation proactive et dialogique des réseaux sociaux est associée à une perception publique plus favorable et à une moindre diffusion de contenus négatifs.

Les résultats relatifs à cette hypothèse sont partiellement confirmatifs, mais appellent une qualification importante liée à la segmentation des publics, peu développée dans la formulation initiale de H3. Claire perçoit sans ambiguïté les réseaux sociaux comme une opportunité lorsqu'ils sont utilisés activement, permettant de « prendre l'initiative de communiquer plutôt que de subir une vague d'informations non maîtrisées » et de répondre directement aux clients inquiets — une description qui recoupe fidèlement le mécanisme de dialogic engagement mis en évidence par Ki et Nekmat (2014). L'exemple donné par Sophie (message rassurant diffusé sur les réseaux sociaux lors d'un incident sur les terminaux de paiement) illustre concrètement ce même mécanisme et confirme, empiriquement, l'intérêt d'une réponse rapide et directe sur ces canaux.

Sophie introduit toutefois une nuance déterminante, absente de la formulation initiale de H3 : l'efficacité des réseaux sociaux dépend fortement du profil démographique du public concerné — dans son cas, une clientèle bancaire jugée peu encline à s'informer en priorité sur ces plateformes, ce qui limite la portée du canal social pour ce type précis d'audience, sans pour autant en invalider l'usage. Isabelle relativise de façon convergente l'idée d'un canal supérieur en soi, insistant sur l'adéquation entre le canal et les habitudes de communication normales de l'organisation plutôt que sur la nature intrinsèquement digitale ou non du canal. Le cas de Julien, enfin, introduit une divergence notable par rapport à l'esprit de H3 : dans un contexte fortement B2B, ce sont des canaux non digitaux et hautement personnalisés — rencontres individuelles des dirigeants avec leurs plus grands clients institutionnels, échelonnées sur plusieurs mois — qui ont constitué le levier de restauration de la confiance le plus mobilisé, les réseaux sociaux n'apparaissant dans son récit que comme un canal secondaire, au bénéfice du communiqué de presse et des relations presse construites en amont.

Ce résultat rejoint et prolonge Schultz, Utz et Göritz (2011), pour qui le médium importe autant sinon davantage que le message : le corpus confirme que le choix du canal constitue une décision stratégique à part entière, mais suggère que ce choix doit être arbitré non seulement en fonction des propriétés intrinsèques de chaque canal (rapidité, portée, caractère dialogique), mais aussi, de façon déterminante, en fonction de la segmentation du public visé — grand public résidentiel ou clientèle institutionnelle à forte valeur, jeune public numérique ou clientèle plus âgée et moins connectée.

Statut de l'hypothèse. H3 est partiellement confirmée. L'usage dialogique et proactif des réseaux sociaux est bien associé, dans le corpus, à une perception plus favorable lorsqu'il touche un public grand public numériquement actif. Ce résultat doit cependant être nuancé par un facteur de segmentation d'audience non prévu dans la formulation initiale de l'hypothèse : pour des publics institutionnels ou peu numériques, des canaux personnalisés non digitaux peuvent s'avérer plus déterminants que les réseaux sociaux dans la restauration de la confiance.

7.2.4 Un constat transversal sur le registre du message (dimension D4)

La dimension D4 — public et registre — ne fait pas l'objet d'une hypothèse dédiée dans le modèle initial, mais les résultats descriptifs y révèlent l'une des convergences les plus fortes et les plus unanimes de l'ensemble du corpus : cinq répondants sur cinq mettent en garde, en des termes variés, contre le langage technique, juridique ou jargonneux, et appellent à un registre simple, clair et compréhensible par tous. Claire résume cette exigence par une série de questions

simples que devrait pouvoir résoudre tout message de crise : qu'est-ce qui s'est passé, qu'est-ce que cela signifie pour vous, y a-t-il une action à entreprendre de votre côté, quelles mesures ont été prises. Isabelle formule un constat structurellement identique en évoquant la nécessité de s'adresser à une audience « de tous horizons ».

Ce constat entre en résonance directe avec un exemple mobilisé dans le cadre théorique de ce mémoire : Cornelissen (2023) analyse le cas Boeing et les crashs du 737 Max comme un exemple de communication défensive et techniciste, insuffisamment humaine, qui a nui à la perception de l'entreprise. La convergence entre cet exemple théorique et le constat unanime du terrain luxembourgeois et belge conforte solidement, sur ce point précis, l'articulation entre clarté du registre et efficacité perçue de la communication de crise, indépendamment du secteur ou du type de crise considéré.

7.2.5 H4 — Action corrective et reconstruction de la confiance (dimension D5)

Rappel de l'hypothèse. H4 postule que les entreprises annonçant et mettant en œuvre des actions correctives concrètes, visibles et cohérentes avec leurs engagements reconstituent leur capital de confiance plus efficacement que celles dont la communication se limite à des déclarations symboliques.

Cette hypothèse est celle qui recueille la convergence la plus large et la plus explicite de l'ensemble du corpus : les cinq répondants et les quatre cas documentés y font tous référence, directement ou indirectement. Marc illustre cette exigence par une approche structurée de type ISO 27001, pilotée par le risque réel plutôt que par l'urgence médiatique ; Julien par une réorganisation substantielle de ses équipes de sécurité et un investissement budgétaire dédié ; Sophie par le déploiement d'un outil de veille détectant les sites frauduleux usurpant l'identité de la banque. Ce constat corrobore directement Gillespie et Dietz (2009), pour qui la reconstruction de la confiance organisationnelle repose sur la démonstration conjointe de la compétence (ability) et de l'intégrité (integrity, benevolence) de l'organisation dans la durée, ainsi que Benoit (1997), pour qui l'action corrective constitue l'une des stratégies les plus robustes de réparation d'image.

L'apport interprétatif le plus original de cette section provient toutefois d'une remarque d'Isabelle qui, sans être reprise en ces termes par les autres répondants, éclaire d'un jour nouveau la lecture de D5 : « si on met en place des actions qui auraient dû être des mesures de base et qu'on ne les avait pas encore, les communiquer après coup peut être perçu comme un aveu de

lacune ». Cette remarque met au jour ce que l'on peut désigner comme un paradoxe de l'aveu de négligence, non anticipé par le modèle de Gillespie et Dietz : communiquer sur une action corrective peut, simultanément, démontrer la compétence retrouvée de l'organisation (effet positif sur la dimension ability) et révéler, en creux, que cette compétence faisait défaut avant la crise (effet négatif sur cette même dimension, rétrospectivement). Ce paradoxe trouve une confirmation empirique frappante dans le cas Free : la CNIL a explicitement retenu, parmi les motifs de sanction, l'absence de mesures de sécurité pourtant qualifiées d'« élémentaires », ce qui signifie que les mesures correctives annoncées après la crise ont pu être lues par le régulateur non comme une preuve de compétence retrouvée, mais comme la reconnaissance a posteriori d'une négligence antérieure — configurant ainsi une trajectoire où l'action corrective, loin de restaurer la confiance, a au contraire aggravé la sanction.

Ce paradoxe invite à nuancer la formulation de H4 : l'action corrective ne produit ses effets positifs sur la confiance que si elle est perçue comme un renforcement volontaire et proportionné, et non comme le simple comblement, sous la contrainte, d'une lacune préexistante et négligée. Cette nuance rejoint, sans s'y réduire tout à fait, la distinction entre crise-accident et crise-transgression évoquée dans le cadre théorique (Cornelissen, 2023, adaptant Coombs, 2007) : une action corrective présentée à la suite d'une crise cadrée comme accident (défaillance imprévisible) est plus susceptible d'être perçue comme un renforcement légitime, alors que la même action, présentée à la suite d'une crise cadrée — ou requalifiée par un tiers, comme un régulateur — en transgression (négligence connue et non traitée), risque de fonctionner comme un aveu rétrospectif.

Statut de l'hypothèse. H4 est confirmée par l'ensemble du corpus, avec un apport interprétatif significatif : la relation entre action corrective et reconstruction de la confiance n'est pas linéaire, mais conditionnée par le cadrage de la crise (accident ou transgression) dans lequel cette action corrective est reçue par les publics et par les régulateurs. Ce paradoxe de l'aveu de négligence constitue l'un des résultats les plus originaux de cette recherche empirique et mériterait d'être approfondi dans des travaux ultérieurs.

7.2.6 Synthèse : statut des quatre hypothèses

Hypothèse	Statut	Principal apport interprétatif
H1 — Transparence et rapidité	Partiellement confirmée	La proactivité suppose une capacité de détection préalable et un délai apprécié contextuellement, non un seuil fixe universel de 72 heures.
H2 — Adéquation stratégique	Confirmée, nuancée dans sa forme	L'accommodation observée est une reconnaissance factuelle et digne de responsabilité, non une excuse émotionnelle au sens plein de l'Image Repair Theory.
H3 — Communication digitale et dialogique	Partiellement confirmée	L'efficacité des réseaux sociaux est conditionnée par la segmentation du public ; les canaux personnalisés non digitaux priment pour les publics institutionnels.
H4 — Action corrective et confiance	Confirmée, avec nuance importante	Paradoxe de l'aveu de négligence : l'effet de l'action corrective sur la confiance dépend du cadrage (accident ou transgression) dans lequel elle est reçue.

7.2.7 Apports empiriques non anticipés par le cadre théorique initial

Au-delà de la mise à l'épreuve directe des quatre hypothèses, l'analyse du corpus fait émerger plusieurs éléments qui n'étaient pas explicitement prévus par le modèle à cinq dimensions construit au chapitre 5, et qui viennent l'enrichir. Le premier est la centralité, dans le discours de trois répondants sur cinq (Marc, Julien, et de façon plus implicite Sophie et Claire à travers la description de leurs cellules de crise), d'une séparation organisationnelle stricte entre une cellule technique, chargée de la remédiation opérationnelle, et une cellule de communication, chargée de la gestion des parties prenantes, les deux étant coiffées par un responsable commun assurant la coordination. Julien va jusqu'à désigner cette séparation comme la leçon la plus importante tirée de sa propre expérience de crise, la première occurrence ayant souffert d'une cellule technique trop mobilisée par la résolution de l'incident pour se consacrer pleinement à

la communication. Cet élément, de nature organisationnelle plutôt que discursive, complète utilement la dimension D2 du modèle, qui porte sur le contenu de la stratégie discursive sans interroger la gouvernance qui la produit.

Le deuxième élément concerne le principe, évoqué indépendamment par Julien et Isabelle, d'une synchronisation stricte entre communication interne et communication externe — les collaborateurs ne devant jamais apprendre par la presse une information que l'organisation ne leur a pas encore communiquée en interne. Ce principe, non présent sous cette forme dans le modèle à cinq dimensions, mériterait d'être intégré comme une composante à part entière de la dimension D3, aux côtés du choix des canaux externes.

Le troisième élément est le rôle de la culture de préparation et de simulation, mentionnée spontanément par Marc (simulations annuelles avec scénarios variés, jusqu'à la fabrication d'une fausse une de journal pour tester les réactions de l'équipe communication), par Sophie (cellule de crise testée par des appels-surprises) et par Isabelle (recommandation de simulations régulières et de révision du plan au moins deux fois par an). Ce résultat suggère que la dimension D1 du modèle, centrée sur la temporalité de la communication elle-même, gagnerait à intégrer un indicateur amont relatif au degré de préparation et d'entraînement de l'organisation, qui conditionne largement sa capacité effective à respecter les délais évoqués en 7.2.1.

Le quatrième élément, déjà relevé en 7.1.2, est le poids différencié des cadres réglementaires sectoriels et nationaux — DORA et CSSF pour les répondants luxembourgeois du secteur financier, obligations de résilience nationale pour Julien dans le secteur des télécommunications belge — qui vient se superposer, et parfois se substituer, au seul cadre générique du RGPD mobilisé dans la formulation initiale de H1. Ce constat invite à une lecture du modèle d'analyse sensible au contexte réglementaire sectoriel, plutôt qu'à une application uniforme du seuil des 72 heures à l'ensemble des organisations.

Enfin, le refus assumé des profils informatiques et cybersécurité (Marc, Julien) de s'exprimer eux-mêmes publiquement, au profit d'équipes communication spécifiquement formées à cet effet, constitue un résultat convergent qui, sans remettre en cause le modèle d'analyse, éclaire sa mise en œuvre concrète : la stratégie discursive (D2) et le registre (D4) qu'il décrit sont, dans les organisations étudiées, presque systématiquement produits par une fonction communication distincte de la fonction technique, cette dernière se limitant à fournir une information factuelle filtrée avant transmission — configuration qui renforce, une fois encore, l'intérêt de la séparation des cellules décrite plus haut.

En synthèse, le matériel empirique recueilli dans le cadre de ce mémoire corrobore, dans ses grandes lignes, le modèle d'analyse à cinq dimensions construit à partir de la SCCT, de l'Image Repair Theory et de la littérature sur la communication corporate et digitale de crise : la transparence rapide, la reconnaissance de responsabilité, l'usage dialogique des canaux et l'action corrective concrète y apparaissent, de façon convergente, comme des déterminants d'une communication de crise jugée efficace par les professionnels interrogés et comme des facteurs discriminants entre les cas de communication les mieux et les moins bien évalués par les autorités de contrôle. La recherche empirique apporte cependant trois nuances substantielles à ce cadre théorique, qui en constituent la principale contribution originale : la nécessité d'articuler la proactivité de la communication à la capacité de détection de l'organisation, la reconnaissance que l'accommodation prescrite par la littérature se traduit, sur le terrain étudié, par une transparence factuelle et digne plutôt que par une excuse au sens plein du terme, et la mise au jour d'un paradoxe de l'aveu de négligence qui vient complexifier la relation, jusqu'ici présentée de façon linéaire dans le cadre théorique, entre action corrective et reconstruction de la confiance.

7.3 Retour sur la méthode et transition

Un retour réflexif sur la méthode s'impose ici, comme le recommande le séminaire d'accompagnement au mémoire : que se serait-il passé avec un plus grand nombre d'entretiens ? Un échantillon plus large aurait sans doute permis de vérifier si les clivages observés entre profils informatiques et profils communication se maintiennent au-delà de cinq personnes, et si le poids du contexte réglementaire luxembourgeois se retrouve dans d'autres environnements nationaux moins régulés. Ces questions restent ouvertes.

Un constat s'impose toutefois déjà au terme de ces cinq entretiens : le degré de convergence observé en 7.1.2 est élevé. Sur la plupart des thèmes du guide, quatre voire cinq répondants sur cinq tiennent des propos très proches, alors même qu'ils exercent dans des secteurs et des fonctions différents. Cette convergence suggère une forme de saturation des données : les principes qui structurent un plan de communication de crise pour une fuite de données semblent largement partagés — communiquer vite sans attendre de tout savoir, séparer la cellule technique de la cellule communication, synchroniser l'interne et l'externe, éviter le jargon, privilégier l'action concrète à la déclaration symbolique. Ces principes ne varient guère d'une organisation mature à l'autre.

Il est donc plausible que des entretiens supplémentaires auraient surtout confirmé et affiné ces constats, plus qu'ils n'auraient révélé des stratégies radicalement nouvelles. Cette lecture doit cependant rester prudente, car une saturation ne se démontre pas formellement sur un échantillon de cinq personnes ; elle est sans doute moins vraie pour des secteurs peu régulés ou pour des organisations moins matures en gestion de crise, non représentées dans ce corpus et où les pratiques sont vraisemblablement plus disparates.

Un design purement quantitatif, tel qu'envisagé initialement à travers le questionnaire exploratoire, aurait par ailleurs permis de mesurer la fréquence de certaines attentes dans le grand public, mais n'aurait pas donné accès aux arbitrages internes qui construisent, en amont, les messages de crise — c'était précisément l'objet de la question de recherche. Le choix d'une démarche qualitative à deux volets apparaît donc cohérent avec l'objet étudié et avec le degré de standardisation des pratiques qu'il a permis de mettre au jour, tout en assumant pleinement les limites de portée qui lui sont inhérentes et qui ont été détaillées en 6.7.

Les résultats présentés dans ce chapitre — le statut nuancé des quatre hypothèses de travail, ainsi que les apports empiriques non anticipés par le cadre théorique initial — constituent la matière sur laquelle s'appuiera la conclusion générale de ce mémoire, qui reviendra sur la question de recherche initiale, discutera la portée et les limites de ces résultats, et formulera des recommandations pratiques à destination des organisations confrontées à une fuite de données.

CONCLUSION GÉNÉRALE

Ce mémoire est parti d'un constat simple : les fuites de données se multiplient, les organisations y sont de plus en plus confrontées, et leur manière de communiquer dans les heures et les semaines qui suivent pèse lourd sur leur réputation et sur la confiance de leurs parties prenantes. De ce constat est née une question de recherche précise : quelle stratégie de communication une entreprise met-elle en place auprès du grand public en cas de fuite de données ? Pour y répondre, ce travail a suivi un cheminement en deux temps, articulant une réflexion théorique et une mise à l'épreuve empirique.

La première partie a construit le socle théorique de la recherche, en mobilisant la communication corporate, la communication de crise, et deux théories de référence : la Situational Crisis Communication Theory de Coombs et l'Image Repair Theory de Benoit. Elle a ensuite examiné la spécificité des fuites de données en tant que crise organisationnelle à part entière — leur nature numérique, leur temporalité parfois décalée, leurs effets réputationnels en cascade — avant de déboucher sur un modèle d'analyse à cinq dimensions et sur quatre hypothèses de travail. La seconde partie a mis ce modèle à l'épreuve du terrain, à travers cinq entretiens semi-directifs menés auprès de professionnels de la sécurité de l'information, de la communication corporate et du conseil en gestion de crise, ainsi qu'à travers quatre cas de communication effectivement observés, dont trois documentés de façon indépendante et sanctionnés ou commentés par une autorité de contrôle.

Les résultats de cette confrontation sont, dans l'ensemble, cohérents avec le cadre théorique mobilisé. La rapidité de la communication reste un facteur déterminant, mais elle dépend d'abord d'une capacité de détection : on ne peut être transparent sur ce que l'on n'a pas encore identifié. La reconnaissance de responsabilité importe davantage que l'excuse elle-même, les professionnels interrogés préférant assumer les faits plutôt que s'excuser au sens plein du terme. L'usage dialogique des réseaux sociaux profite d'abord aux publics grand public, actifs sur ces plateformes, tandis que pour des publics institutionnels ou à forte valeur, les canaux personnalisés restent souvent plus efficaces. L'action corrective demeure, enfin, le levier le plus consensuel de reconstruction de la confiance, à condition qu'elle ne soit pas perçue comme l'aveu tardif d'une négligence déjà connue — ce dernier point constituant sans doute l'apport le plus original de ce mémoire. Le paradoxe de l'aveu de négligence n'était pas anticipé par le cadre théorique initial ; il éclaire pourtant un mécanisme central, selon lequel une même action

corrective peut renforcer la confiance ou l'éroder, tout dépendant du cadrage de la crise dans lequel elle est reçue, accident ou transgression.

Au-delà de sa contribution théorique, ce travail permet de dégager quelques recommandations concrètes à destination des organisations confrontées à une fuite de données. Il s'agit d'abord de se préparer avant la crise et non pendant : un plan de crise documenté, testé et révisé régulièrement change concrètement l'issue d'un incident. Il s'agit ensuite de séparer la cellule technique de la cellule de communication, sous une coordination commune, et de synchroniser systématiquement la communication interne et la communication externe, afin que les collaborateurs n'apprennent jamais une information par la presse. Il convient également de communiquer vite, mais de façon complète — une seule communication structurée valant mieux que plusieurs vagues confuses —, dans un registre simple et clair, sans jargon technique ni juridique, et d'assumer les faits sans s'excuser de façon excessive ni théâtrale. Enfin, et c'est sans doute la recommandation la plus directement issue de ce mémoire, il est essentiel de ne jamais communiquer une action corrective sans avoir anticipé la question qu'elle soulève implicitement : pourquoi cette mesure n'existait-elle pas avant la crise ?

Ce mémoire comporte des limites, assumées et déjà discutées au fil du texte. L'échantillon reste restreint, avec cinq entretiens et quatre cas, et il est aussi situé géographiquement et sectoriellement, entre le Luxembourg et la Belgique, dans des secteurs financier et régulé pour l'essentiel. Les résultats ne prétendent donc pas à une représentativité statistique ; ils offrent une lecture qualitative, argumentée et triangulée, mais circonscrite à ce terrain précis. Plusieurs pistes de recherche s'en dégagent naturellement : élargir le corpus à d'autres secteurs moins régulés pour vérifier si les mêmes principes s'y retrouvent, interroger directement les publics touchés par une fuite de données plutôt que les seules organisations, pour confronter le discours produit à sa réception réelle, ou encore approfondir le paradoxe de l'aveu de négligence, qui mériterait une étude dédiée au croisement de la communication de crise et de la théorie de la confiance organisationnelle.

Un dernier constat s'impose, en guise de mot de la fin. La fuite de données n'est plus un risque exceptionnel ; elle est devenue, pour beaucoup d'organisations, une question de moment plutôt que de probabilité. Dans ce contexte, la communication de crise n'est plus un exercice secondaire réservé à l'urgence : elle devient une compétence organisationnelle à part entière, une compétence qui se prépare, se teste et s'incarne bien avant que la crise n'éclate.

BIBLIOGRAPHIE

Arpan, L. M., & Roskos-Ewoldsen, D. R. (2005). Stealing thunder: An analysis of the effects of proactive disclosure of crisis information. *Public Relations Review*, 31(3), 425–433.

Benoit, W. L. (1997). Image repair discourse and crisis communication. *Public Relations Review*, 23(2), 177–186.

Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. (2013). Digital business strategy: Toward a next generation of insights. *MIS Quarterly*, 37(2), 471–482.

Catellani, A., Sauvajol-Rialland, C., & Allard-Huver, F. (2022). *Les relations publiques*. Dunod.

Chung, S., & Lee, S. (2021). Crisis management and corporate apology: The effects of causal attribution and apology type on publics' cognitive and affective responses. *International Journal of Business Communication*, 58(1), 125–144.

Claeys, A.-S., Cauberghe, V., & Vyncke, P. (2010). Restoring reputations in times of crisis: An experimental study of the Situational Crisis Communication Theory and the moderating effects of locus of control. *Public Relations Review*, 36(3), 256–262.

Commission nationale de l'informatique et des libertés. (2024, 8 mars). France Travail : la CNIL enquête sur la fuite de données et donne des conseils pour se protéger. *CNIL*. https://www.cnil.fr/fr/france-travail-la-cnil-enquete-sur-la-fuite-de-donnees-et-donne-des-conseils-pour-se-proteger

Commission nationale de l'informatique et des libertés. (2026a, 8 janvier). Délibération SAN-2026-001 de la formation restreinte prononçant une sanction pécuniaire à l'encontre de la société FREE MOBILE. *Légifrance*. https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000053352664

Commission nationale de l'informatique et des libertés. (2026b, 8 janvier). Délibération SAN-2026-002 de la formation restreinte prononçant une sanction pécuniaire à l'encontre de la société FREE. *Légifrance*. https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000053352643

Commission nationale de l'informatique et des libertés. (2026c, 13 janvier). Violation de données : sanction de 42 millions d'euros à l'encontre des sociétés FREE MOBILE et FREE. *CNIL*. https://www.cnil.fr/fr/sanction-free-2026

Commission nationale de l'informatique et des libertés. (2026d, 22 janvier). Violation de données : sanction de 5 millions d'euros à l'encontre de FRANCE TRAVAIL. *CNIL*. https://www.cnil.fr/fr/violation-de-donnees-sanction-5millions-france-travail

Coombs, W. T. (1995). Choosing the right words: The development of guidelines for the selection of the “appropriate” crisis-response strategies. *Management Communication Quarterly*, 8(4), 447–476.

Coombs, W. T. (2007). Protecting organization reputations during a crisis: The development and application of situational crisis communication theory. *Corporate Reputation Review*, 10(3), 163–176.

Coombs, W. T. (2015). The value of communication during a crisis: Insights from strategic communication research. *Business Horizons*, 58(2), 141–148.

Coombs, W. T., & Holladay, S. J. (2002). Helping crisis managers protect reputational assets. *Management Communication Quarterly*, 16(2), 165–186.

Cornelissen, J. (2023). *Corporate communication: A guide to theory and practice* (7e éd.). SAGE Publications.

Doorley, J., & Garcia, H. F. (2015). *Reputation management: The key to successful public relations and corporate communication* (3e éd.). Routledge.

Erickson, S. L., Stone, M., Serdar, G., & Pfeffer, B. (2023). When crisis victims are not customers: SCCT and the Equifax data breach. *Journal of Managerial Issues*, 35(2).

France Travail. (2026, 22 janvier). France Travail prend acte de la sanction de la CNIL et rappelle que la cybersécurité et la protection des données sont des enjeux prioritaires. *France Travail*. https://www.francetravail.org/accueil/communiques/2026/france-travail-prend-acte-de-la-sanction-de-la-cnil-et-rappelle-que-la-cybersecurite-et-la-protection-des-donnees-sont-des-enjeu.html

Gillespie, N., & Dietz, G. (2009). Trust repair after an organization-level failure. *Academy of Management Review*, 34(1), 127–145.

Goode, S., Hoehle, H., Venkatesh, V., & Brown, S. A. (2017). User compensation as a data breach recovery action: An investigation of the Sony PlayStation Network breach. *MIS Quarterly*, 41(3), 703–727.

Hearit, K. M. (2006). *Crisis management by apology: Corporate response to allegations of wrongdoing*. Lawrence Erlbaum Associates.

INCYBER News. (2024, 16 septembre). Boulanger et Cultura victimes d'une fuite de données. *INCYBER News*. https://incyber.org/article/boulanger-cultura-victimes-fuite-donnees/

Jin, Y., Liu, B. F., & Austin, L. L. (2014). Examining the role of social media in effective crisis management. *Communication Research*, 41(1), 74–94.

Ki, E.-J., & Nekmat, E. (2014). Situational crisis communication and interactivity: Usage and effectiveness of Facebook for crisis management by Fortune 500 companies. *Computers in Human Behavior*, 35, 140–147.

Kim, B., Johnson, K., & Park, S.-Y. (2017). Lessons from the five data breaches: Analyzing framed crisis response strategies and crisis severity. *Cogent Business & Management*, 4(1), Article 1354525.

Kim, S., Avery, E. J., & Lariscy, R. W. (2009). Are crisis communicators practicing what we preach? An evaluation of crisis response strategy analyzed in public relations research from 1991 to 2009. *Public Relations Review*, 35(4), 446–448.

Knight, R., & Nurse, J. R. C. (2020). A framework for effective corporate communication after cyber security incidents. *Computers & Security*, 99, Article 102036.

Kuipers, S. L., & Schonheit, M. (2022). Data breaches and effective crisis communication: A comparative analysis of corporate reputational crises. *Corporate Reputation Review*, 25(3), 176–197.

Le Monde Informatique. (2024, 9 septembre). Piratage de Boulanger : des centaines de milliers de clients touchés. *Le Monde Informatique*. https://www.lemondeinformatique.fr/actualites/lire-piratage-de-boulanger-des-centaines-de-milliers-de-clients-touches-94654.html

Lee, B. K. (2004). Audience-oriented approach to crisis communication: A study of Hong Kong consumers' evaluation of an organizational crisis. *Communication Research*, 31(5), 600–618.

Libaert, T. (2017). *Le plan de communication* (5e éd.). Dunod.

Libaert, T. (2020a). *La communication de crise* (5e éd.). Dunod.

Libaert, T. (2020b). *La communication externe des entreprises* (5e éd.). Dunod.

Libaert, T., & Johannes, K. (2016). *La communication corporate*. Dunod.

Loucif, S. (2014). La confiance comme instrument d'analyse et de compréhension des relations publiques. *Revue Algérienne de la Communication*, 16(2), 29–48.

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing*, 81(1), 36–58.

Parlement européen et Conseil de l'Union européenne. (2016). Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données). *Journal officiel de l'Union européenne*, L119.

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, 2(2), 121–135.

Ruohonen, J., Hjerppe, K., & Kortesuo, K. (2024). *Crisis communication in the face of data breaches*. arXiv. https://doi.org/10.48550/arXiv.2406.01744

Schultz, F., Utz, S., & Göritz, A. (2011). Is the medium the message? Perceptions of and reactions to crisis communication via Twitter, blogs and traditional media. *Public Relations Review*, 37(1), 20–27.

Sinanaj, G., Muntermann, J., & Cziesla, T. (2015). How data breaches ruin firm reputation on social media! Insights from a sentiment-based event study. In *Wirtschaftsinformatik Proceedings 2015* (Paper 61).

Syed, R. (2019). Enterprise reputation threats on social media: A case of data breach framing. *The Journal of Strategic Information Systems*, 28(3), 257–274.

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, 34(1), 134–153.

Usine Digitale. (2024, 9 septembre). Cybersécurité : Boulanger victime d'une fuite de données, des millions de Français concernés. *Usine Digitale*. https://www.usine-digitale.fr/article/cybersecurite-boulanger-victime-d-une-fuite-de-donnees-des-millions-de-francais-concernes.N2218196

Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems*, 28(2), 118–144.

Wang, P., & Park, S. (2017). Communication in cybersecurity: A public communication model for business data breach incident handling. *Issues in Information Systems*, 18(2), 136–147.

ANNEXES

Annexe 1 . GUIDE D'ENTRETIEN

« Quelle stratégie de communication une entreprise met-elle en place auprès du grand public en cas de fuite de données ? »

Profils d'interviewés ciblés

- Directeurs / Responsables de la communication (Directeur communication, PR Manager)
- Responsables informatiques et cybersécurité (CIO, DSI)
- Managing Directors / Directeurs généraux avec expertise en communication de crise

Durée estimée	45 à 60 minutes
Type	Entretien semi-directif — enregistrement audio avec accord préalable
Anonymat	Garanti sur demande — données utilisées exclusivement dans le cadre du mémoire
Diffusion	Aucun élément publié sans approbation — le mémoire final vous sera transmis

Introduction à présenter à l'interviewé(e)

Bonjour et merci de m'accorder de votre temps. Je suis étudiant en Master 2 en communication, finalité Communication stratégique des organisations, à l'Université catholique de Louvain (UCLouvain).

Mon mémoire porte sur les stratégies de communication déployées par les entreprises lors d'une fuite de données. Face à la multiplication des cyberattaques et aux exigences du RGPD, cette question est devenue centrale pour toute organisation gérant des données personnelles.

Votre expertise est précieuse pour ma recherche. Cet entretien est confidentiel : vos propos seront utilisés uniquement à des fins académiques, sous anonymat si vous le souhaitez, et aucun élément ne sera publié sans votre accord. L'entretien durera environ 45 à 60 minutes. Il n'y a pas de bonnes ou de mauvaises réponses — c'est votre point de vue et votre expérience qui m'intéressent.

Puis-je enregistrer notre échange pour faciliter la retranscription ?

AXE 1 — Profil et contexte

Q1	**Pouvez-vous me présenter votre parcours et votre rôle actuel ? Êtes-vous régulièrement confronté(e) à des problématiques de communication de crise ou de sécurité des données ?**
Relances	→ *Depuis combien de temps occupez-vous ce poste ?* → *Avez-vous déjà travaillé dans d'autres secteurs ou organisations ?* → *Y a-t-il une cellule de crise ou une équipe dédiée à ces enjeux dans votre organisation ?*

Q2	**Comment votre organisation perçoit-elle aujourd'hui le risque d'une fuite de données ? Est-ce un sujet qui a pris de l'importance ces dernières années ?**
Relances	→ *Y a-t-il eu des incidents récents dans votre secteur qui ont changé la manière dont vous abordez ce risque ?* → *La direction générale est-elle sensibilisée à la dimension communicationnelle de ce risque, au-delà de la dimension purement technique ?*

AXE 2 — La fuite de données comme crise communicationnelle

Q3	**Selon vous, en quoi une fuite de données constitue-t-elle une crise particulière pour une organisation ? Quels sont ses impacts les plus significatifs sur la réputation et la confiance ?**
Relances	→ *Pensez-vous que la cause de la fuite — une négligence interne ou une attaque externe — change la manière dont le public réagit et attribue les responsabilités ?* → *Avez-vous observé des situations où une fuite de données a eu des effets négatifs au-delà des clients directement touchés ?* → *Y a-t-il selon vous des secteurs plus vulnérables que d'autres à ces impacts réputationnels ?*
Lien H	*H1 et H2 : lien entre type de crise, attribution de responsabilité et ampleur des dommages réputationnels*

Q4	**Avez-vous été confronté(e) à une fuite de données — dans votre organisation ou dans une organisation avec laquelle vous avez collaboré ? Comment la situation a-t-elle été gérée sur le plan communicationnel ?**
Relances	→ *Quelles ont été les premières décisions prises en matière de communication ? Qui les a prises ?* → *Quelles ont été les réactions du public et des médias ? Y a-t-il eu des moments où la situation a échappé au contrôle communicationnel ?* → *Si vous n'avez pas vécu de fuite directement : quel cas de gestion de crise — réussie ou ratée — vous a le plus marqué ? Pourquoi ?*
Lien H	*Toutes dimensions du modèle*

AXE 3 — Temporalité et stratégie de communication

Q5	**À quel moment et dans quel délai une organisation devrait-elle communiquer publiquement après la découverte d'une fuite de données ? Faut-il attendre d'avoir toutes les informations, ou vaut-il mieux prendre la parole rapidement quitte à compléter l'information ultérieurement ?**
Relances	→ *Le RGPD impose une notification aux autorités dans les 72 heures — cela vous paraît-il réaliste en pratique ? Qui décide du moment de la communication publique dans votre organisation ?* → *Que pensez-vous de la stratégie qui consiste pour une organisation à révéler elle-même la fuite avant que les médias ou des tiers ne le fassent ? Quels en sont selon vous les avantages et les risques ?* → *Avez-vous des exemples d'organisations qui ont bien géré cette dimension temporelle ? Et des contre-exemples ?*
Lien H	*H1 : stealing thunder, temporalité, conformité RGPD — D1 du modèle*

Q6	**Quel contenu et quel ton une organisation devrait-elle adopter dans ses communications officielles après une fuite ? Comment trouver le bon équilibre entre reconnaître sa responsabilité et protéger ses intérêts légaux et réputationnels ?**
Relances	→ *Faut-il selon vous présenter des excuses publiques ? Y a-t-il une différence entre dire 'nous sommes désolés que cela se soit produit' et 'nous assumons notre responsabilité et nous engageons à...' ?* → *Les équipes juridiques freinent-elles souvent ces déclarations ? Comment gérez-vous cette tension entre le service juridique et le service communication ?* → *Y a-t-il des formulations ou des postures que vous considérez comme des erreurs à éviter absolument ?*
Lien H	*H2 : stratégies accommodatives vs défensives, excuses responsibility-oriented vs sympathy-oriented — D2 et D4*

Q7	**Quels canaux de communication privilégiez-vous pour informer le public lors d'une fuite de données ? Pensez-vous que le choix du canal — communiqué de presse, réseaux sociaux, email direct aux clients — influence la manière dont le message est reçu ?**
Relances	→ *Les réseaux sociaux sont-ils selon vous une opportunité ou un risque supplémentaire en situation de crise ?* → *Pensez-vous qu'il est utile de répondre directement aux commentaires et questions des internautes sur les réseaux sociaux lors d'une crise ? Pourquoi ?* → *Comment garantir la cohérence des messages entre tous les canaux lorsqu'on est sous pression ?*
Lien H	*H3 : rôle des médias sociaux et communication dialogique — D3 du modèle*

AXE 4 — Reconstruction de la confiance et actions post-crise

Q8	**Au-delà de la communication immédiate, quelles actions concrètes une organisation devrait-elle mettre en place après une fuite de données pour démontrer qu'elle a tiré les leçons de l'incident et pour reconstruire la confiance de ses parties prenantes ?**
Relances	*→ Quelle importance accordez-vous aux offres de compensation aux personnes affectées — services de surveillance de crédit, remboursements, gestes commerciaux ?* *→ Un audit de sécurité indépendant communiqué publiquement vous paraît-il efficace pour restaurer la confiance ?* *→ Combien de temps faut-il selon vous pour reconstruire une réputation significativement endommagée par une fuite de données ?*
Lien H	*H4 : action corrective, cohérence discours/actes, reconstruction de la confiance — D5 du modèle*

Q9	**Votre organisation dispose-t-elle d'un plan de communication spécifiquement prévu pour les fuites de données ou les cyberattaques ? Si oui, comment est-il structuré et qui est impliqué dans sa conception et son activation ?**
Relances	*→ Ce plan est-il régulièrement testé ou mis à jour ?* *→ Qui sont les porte-paroles désignés en cas de crise cyber ? Le PDG prend-il la parole directement ?* *→ Si vous n'en avez pas : pensez-vous qu'une telle préparation est nécessaire ? Quels obstacles s'y opposent dans la pratique ?*
Lien H	*H1 et H4 : préparation préalable comme condition de rapidité et d'efficacité — D1 et D5*

AXE 5 — Synthèse et recommandations

Q10	**Si vous deviez conseiller une organisation qui vient de découvrir une fuite de données significative, quelles seraient vos trois recommandations prioritaires en matière de communication ? À l'inverse, quelles sont selon vous les erreurs les plus fréquentes et les plus coûteuses à éviter ?**
Relances	*→ Existe-t-il une 'bonne pratique' qui se démarque dans les cas de gestion de crise cyber que vous avez observés ?* *→ Pensez-vous que les pratiques de communication en cas de fuite de données ont évolué ces dernières années ? Dans quel sens ?* *→ Y a-t-il une question que vous vous posez vous-même sur ce sujet et à laquelle vous n'avez pas encore de réponse ?*
Lien H	*Synthèse H1, H2, H3, H4 — toutes dimensions du modèle*

Clôture de l'entretien

Nous arrivons au terme de cet entretien. Je vous remercie chaleureusement pour la qualité de vos réponses — elles apportent une valeur considérable à ma recherche.

Souhaitez-vous ajouter quelque chose que nous n'aurions pas abordé, ou revenir sur un point qui vous semble particulièrement important ?

Y a-t-il une personne de votre réseau que vous me recommanderiez de rencontrer dans le cadre de cette recherche ?

Le mémoire final vous sera transmis à sa publication. N'hésitez pas à me contacter si vous souhaitez relire les extraits vous concernant avant la finalisation.

Tableau de correspondance — questions, hypothèses et dimensions analytiques

Outil de codage pour l'analyse des entretiens.

Q	Thème	Dimensions	Hypothèses	Profils prioritaires
1–2	Profil et contexte	Toutes	—	Tous
3	Fuite comme crise — impacts	D1, D4	**H1, H2**	Tous
4	Expérience vécue	D1, D2, D3, D4, D5	**H1, H2, H3, H4**	Tous
5	Temporalité — stealing thunder	D1	**H1**	Communication, IT
6	Stratégie discursive — excuses	D2, D4	**H2**	Communication, Management
7	Canaux — réseaux sociaux	D3	**H3**	Communication, Management
8	Actions post-crise — confiance	D5	**H4**	Tous
9	Plan de crise — préparation	D1, D5	**H1, H4**	Communication, IT
10	Synthèse — recommandations	Toutes	**H1, H2, H3, H4**	Tous

Annexe 2. Retranscriptions des entretiens

Entretien 1 — Antoine Leblais

Chief Information Security Officer (CISO) d'une compagnie d'assurance luxembourgeoise

Interviewer : *Pouvez-vous vous présenter, votre parcours et votre rôle actuel ?*

Interviewé(e) : Je m'appelle Antoine Leblais, je suis responsable de la sécurité de l'information du Groupe Foyer. J'ai eu cette opportunité dans le cadre du rachat de la société Globality Health par le Groupe Foyer. Au sein de Globality, j'occupais déjà ce rôle, en plus de celui de DPO — ce dernier rôle n'est plus le mien aujourd'hui, mais j'en conserve une bonne connaissance.

Cela fait maintenant 14 ans que je travaille au Luxembourg. Avant ça, j'ai passé trois ans en Amérique latine, au Chili, pour gérer les opérations de la Loterie nationale chilienne, dans le cadre duquel j'ai mené un projet de certification ISO 27001. Nous avons également ce projet en cours au sein du Groupe Foyer. Et encore avant, j'ai fait du support technique dans le secteur des jeux de hasard — casinos et loteries — à Monaco, pendant six ans. J'ai 46 ans, je suis marié et j'ai un enfant.

Interviewer : *Êtes-vous régulièrement confronté à des problématiques de communication de crise ou de sécurité des données ?*

Interviewé(e) : La communication de crise, assez rarement, car je considère que nous disposons d'une sécurité technique suffisamment robuste pour éviter les crises. Néanmoins, ça arrive. L'an dernier, par exemple, le principal opérateur de téléphonie du Luxembourg a subi une cyberattaque, avec des impacts sur à peu près tous les acteurs luxembourgeois. Comme cet opérateur — la Poste Luxembourg — est en situation de monopole, quand la Poste ne fonctionne plus, rien ne fonctionne. Nous avons donc dû déclencher une simulation de crise. Mais ce n'est pas mensuel : c'est plutôt une fois par an.

Interviewer : *Comment votre organisation perçoit-elle aujourd'hui le risque de fuite de données ? Est-ce un sujet qui a pris de l'importance ces dernières années ?*

Interviewé(e) : Oui, clairement, depuis quelques années. Plusieurs éléments sont entrés en ligne de compte. D'abord, les occurrences : il y a une recrudescence des cyberattaques détectées. Je pense qu'avant il y en avait autant, mais qu'on les détectait moins. Maintenant on les détecte mieux, donc on est plus alerté.

Ensuite, il y a l'avènement de DORA — le Digital Operational Resilience Act —, un règlement européen qui oblige les entités financières et assurancielles comme nous à garantir à leurs clients un minimum de résilience numérique. Si on ne donne pas ces garanties, nos dirigeants s'exposent à des sanctions pénales. Il y a donc un certain niveau de stress autour de ça. Il y a aussi le RGPD, entré en vigueur en 2018, qui inclut des responsabilités pour nos dirigeants, sans compter les pénalités financières. Et puis il y a les risques réputationnels, les risques légaux et les risques business.

Enfin, il y a l'intelligence artificielle. C'est un sujet sur lequel j'interviens d'ailleurs demain lors d'un grand événement tech au Luxembourg. L'IA nous offre des opportunités commerciales incroyables, mais elle est aussi au service des attaquants. Il ne faut pas perdre ça de vue, et c'est quelque chose que nous ne perdons jamais de vue.

Interviewer : *Avez-vous déjà observé des situations où une fuite de données a eu des effets négatifs au-delà des clients directement touchés ? Chez Foyer ou dans vos postes précédents ?*

Interviewé(e) : Sans nommer d'organisations, il est déjà arrivé qu'une machine soit compromise. Cette machine a ensuite été utilisée à distance par des attaquants pour envoyer du phishing via une adresse e-mail légitime. Pour être clair : si mon PC se fait pirater et est laissé à la merci d'un attaquant, celui-ci peut utiliser ma boîte mail officielle pour envoyer des spams ou des tentatives de phishing à grande échelle. C'est arrivé. Nous avons bien évidemment réagi immédiatement.

Mais il faut savoir qu'en sécurité de l'information, on réagit selon trois paradigmes : la confidentialité des données, bien sûr, mais aussi l'intégrité — une donnée corrompue représente le même type de risque qu'une donnée qui aurait fuité — et enfin la disponibilité des données, qui constitue un risque majeur pour le business si les données deviennent inaccessibles. Ce dernier point m'est arrivé à Santiago, avec un crash de base de données — intentionnel ou non, c'est encore incertain à ce jour — il y a 15 ans.

En résumé, les risques sont les mêmes : impact réputationnel majeur, impact business. C'est pourquoi il est important d'avoir une approche structurée de type ISO 27001, qui permet d'agir en fonction du risque réel présenté.

Interviewer : *Suite à ces incidents, quelles ont été les réactions du public ou des médias ? Y a-t-il eu des moments où la situation a pu vous échapper ?*

Interviewé(e) : Non, je n'ai pas eu cette expérience, heureusement. En revanche, ce que nous faisons chez Foyer, c'est de la simulation. Chaque année, nous simulons une crise — une crise locale qui évolue en crise groupe — et nous mettons nos équipes à contribution pour tester leurs compétences. Je n'ai donc jamais eu à déclencher de communication d'excuse ou de gestion de crise publique dans ma carrière.

Je me souviens d'un exercice particulièrement marquant : une année, nous avons mené une simulation sans prévenir l'équipe communication. Nous avons même fabriqué une fausse une de journal titrant sur une cyberattaque massive contre le Groupe Foyer. La responsable communication était en panique totale. On lui a dit de se détendre, que c'était un test. Elle a changé de couleur — mais globalement, ses réactions étaient très bonnes. Ce genre d'exercice permet vraiment de conscientiser les gens. On voit que nous sommes quand même bien entraînés pour gérer ce type de situation.

Interviewer : *Selon vous, quel contenu et quel ton votre département devrait-il adopter dans les communications officielles après une fuite de données ?*

Interviewé(e) : Pour être précis, nous ne réagissons pas publiquement. L'intérêt d'une organisation en cellules de crise, c'est que chacun a son rôle. Il y a d'abord l'équipe de sécurité opérationnelle, ceux qui font le travail technique : restauration des backups, etc. Ensuite, il y a la deuxième ligne de défense, notre niveau, qui est en charge d'évaluer les risques et de faire le pont entre la direction et les équipes techniques. Et enfin, il y a l'équipe communication : c'est leur métier.

Moi, je n'irai certainement pas répondre à la presse. Ce n'est pas mon rôle, et notre équipe n'est pas formée pour ça, car ce n'est pas dans nos attributions. On risquerait de dire un mot de travers, la presse s'en emparerait, et ce serait terminé. Chacun son métier : la communication doit être extrêmement cadrée et confiée uniquement aux équipes qui y sont formées.

Même quand je donne des interviews — comme maintenant, dans un contexte différent —, si c'est destiné à être publié, j'ai un droit de regard au même titre que la communication institutionnelle de l'entreprise. Il faut faire attention aux gens qui pourraient mal interpréter ou déformer les propos.

Interviewer : *Avez-vous un plan préétabli à suivre en cas de fuite de données, et en quoi consiste-t-il ?*

Interviewé(e) : Oui, nous avons un plan de crise. C'est obligatoire dans le cadre de la certification ISO 27001 et de la conformité à DORA. C'est d'ailleurs ce que nous testons

chaque année, selon des scénarios différents : ransomware, intrusion physique, fuite de données massive et discrète, etc. Nous faisons appel à des prestataires spécialisés pour imaginer ces scénarios et évaluer nos réactions — est-ce qu'on entre en mode panique ou en mode structuré ?

Nous avons une documentation qui précise quoi faire, quand le faire, et surtout qui fait quoi. La clé, c'est justement ça : ceux qui doivent communiquer communiquent, ceux qui doivent travailler techniquement travaillent. C'est extrêmement formalisé, car plus on est préparé et organisé, moins la crise a d'impact.

Interviewer : *Si vous deviez conseiller une organisation qui vient de découvrir une fuite de données, quelles seraient vos trois recommandations principales ?*

Interviewé(e) : Premièrement, juguler la crise en gardant son sang-froid.

Deuxièmement, disposer d'un plan de crise documenté et le suivre.

Troisièmement, connaître parfaitement les obligations légales qui incombent à l'entreprise pour déclarer les fuites de données et les incidents dans les délais légaux — car si on ne le fait pas, on ajoute une crise à la crise.

Interviewer : *À l'inverse, quelles sont selon vous les erreurs les plus fréquentes et les plus coûteuses à éviter ?*

Interviewé(e) : La panique, d'abord — c'est humain. Une erreur que la direction peut commettre, c'est de mettre une pression insurmontable sur les équipes techniques, ce qui dessert la cause plutôt qu'autre chose.

Ensuite, penser que ça n'arrive qu'aux autres. Ce n'est pas vrai. La question n'est pas de savoir si on sera attaqué un jour, mais quand. Il faut anticiper, documenter un plan de crise et s'entraîner dessus.

Interviewer : *Comment qualifieriez-vous les relations entre votre département et la communication ? Et quelles informations pouvez-vous transmettre à la communication lors d'une fuite de données ?*

Interviewé(e) : Les relations entre la com et nous sont très bonnes. Le Groupe Foyer est une entreprise avec une longue histoire au Luxembourg, on se connaît tous très bien, et il n'y a pas de conflits entre les équipes. On est plutôt à l'aise sur ce sujet.

Cela dit, pour éviter que la com ne sorte une maladresse dans la presse — parce qu'ironiquement, c'est moi qui risquerais davantage de dire quelque chose d'inapproprié, c'est d'ailleurs pour ça qu'ils sont là — ce qu'on pourrait leur transmettre, c'est : des informations de date et d'heure d'indisponibilité, un état de la situation avec une estimation du moment de retour à la normale. Mais toujours avec la diplomatie qui caractérise les équipes communication, c'est-à-dire sans rien promettre tant qu'il n'y a pas de certitude. Dans ma position d'interface entre les équipes techniques et la com, je filtrerais déjà l'information issue des techniciens avant de la transmettre.

Interviewer : *Et vos relations avec le service juridique ?*

Interviewé(e) : Le DPO est rattaché au service juridique, nous sommes plutôt côté cybersécurité. Les relations avec le juridique, ce n'est pas tous les jours, car on ne parle pas toujours le même langage. Nous avons tendance à trancher entre un "oui" ou un "non" face à une question réglementaire, là où un avis juridique sera beaucoup plus nuancé, pesant les risques de chaque option, sans jamais s'engager totalement. C'est le propre des services juridiques partout dans le monde.

Cela peut générer des frustrations. Néanmoins, ce que nous essayons de faire, c'est de constituer des comités mixtes : quand il y a une initiative portée par un métier de l'assurance, nous nous mettons tous autour d'une table pour évaluer ensemble le risque juridique, le risque cyber, le risque réputationnel, etc. On collabore beaucoup, même si on ne parle pas toujours la même langue.

Interviewer : *Y a-t-il eu des incidents récents dans votre secteur qui ont changé la manière dont vous abordez ce risque ?*

Interviewé(e) : Oui, plusieurs. Sans nommer toutes les organisations, il y en a un qui est très connu sur la place : une attaque de type "insider", c'est-à-dire quelqu'un qui a perdu pied en interne, disposait de droits administrateurs et a tout détruit, y compris les backups. Ça fait réfléchir. Quand une grande organisation subit ce type d'attaque, on se pose des questions sur la façon dont on gère nos droits d'accès. Cela nous a incités à renforcer ce qu'on appelle l'IAM — Identity and Access Management.

Deuxième cas : la fraude au président, un grand classique des dernières années. C'est mon cheval de bataille : je ne veux absolument pas lâcher ce sujet, je veux même le renforcer encore davantage.

Il y a aussi des fuites de données massives dans d'autres secteurs — je pense notamment à Noam —, qui nous ont poussés à renforcer nos pratiques de chiffrement. Globalement, celui qui ne subit pas d'incident s'inspire de ceux qui en subissent pour améliorer sa sécurité. En ce moment, les sujets liés à l'IA sont très prégnants : j'ai vu une entreprise dépenser 500 millions de dollars de tokens en une seule journée chez Claude, parce que les développeurs veulent aller vite. Il faut affiner ces pratiques pour trouver le bon équilibre entre rapidité et prudence.

Entretien 2 — Frederic Jonard

Deputy Chief Information Officer (DCIO) d'un des principaux acteurs du secteur des télécommunications en Belgique

Interviewer : *Pouvez-vous me présenter votre parcours et votre rôle actuel ?*

Interviewé(e) : Je suis chez Orange depuis 30 ans, c'est l'intégralité de ma carrière. J'ai passé la première partie côté business, marketing et opérations métier. Depuis maintenant presque 20 ans, je suis dans le département IT, et je suis actuellement le bras droit du directeur informatique — ce qu'on appelle le Deputy CIO.

Interviewer : *Êtes-vous régulièrement confronté à des problèmes de communication de crise ou de sécurité des données ?*

Interviewé(e) : Heureusement non. Par contre, côté IT, nous avons mis énormément de systèmes en place pour sécuriser au maximum les données que nous traitons — surveiller les flux entrants et sortants, détecter les volumes anormaux sur le réseau, etc.

Mais le périmètre informatique d'une société comme la nôtre est tellement vaste qu'il est toujours difficile de surveiller 100 % de ce qui se passe. Ce que nous savons, c'est qu'une fuite de données peut arriver, aussi bien qu'on se protège. Ce qui est extrêmement important, c'est donc de protéger les données, mais aussi d'avoir un processus de gestion de crise robuste pour le jour où cela arrive.

Interviewer : *Comment votre entreprise perçoit-elle aujourd'hui le risque d'une fuite de données ? Est-ce que ça a pris de l'ampleur ces dernières années ?*

Interviewé(e) : Ça a pris beaucoup d'ampleur, surtout depuis le moment où nous l'avons vécu. Je ne sais pas si vous avez suivi la presse. L'entreprise a quand même fortement réagi à l'échelle du groupe : nous n'étions pas les seuls concernés — deux entités du groupe ont été touchées, dont Orange France. Et même si ce sont des sociétés indépendantes avec des départements informatiques totalement distincts, ça reste Orange. Quand ce phénomène se répète au sein d'un même groupe, ça marque.

Suite à ça, nous avons renforcé notre plan d'investissement pour la sécurisation des données au sens très large — données clients, mais aussi données techniques. Il faut savoir qu'en tant qu'opérateur de télécommunications, nous sommes considérés comme

un opérateur critique : les télécommunications, c'est essentiel au fonctionnement d'un pays.

Aujourd'hui, dans un monde de plus en plus incertain, le niveau de menace est très élevé. On voit des risques allant jusqu'à des attaques étatiques, des tentatives de prise de contrôle de réseaux entiers. C'est d'ailleurs arrivé au Luxembourg, où pendant quelques heures un réseau a été piraté.

Interviewer : *Suite à la cyberattaque que vous avez subie, quels ont été les impacts les plus significatifs sur la réputation et la confiance de vos parties prenantes ?*

Interviewé(e) : Ce qui est extrêmement important, c'est la manière de gérer la crise et la communication. Nous avions deux cellules distinctes : une cellule technique, qui analyse l'incident et définit les plans de remédiation, et une cellule de communication, qui gère toutes les parties prenantes.

Côté communication externe, ce qui se passe dans ce type de situation, c'est qu'on entre assez rapidement en contact avec des interlocuteurs de confiance dans la presse — des journalistes avec qui on entretient une relation — pour donner de l'information en avance, en leur demandant de ne pas communiquer immédiatement. Ça permet de maîtriser la situation : si la moindre information risque de partir hors contrôle, on peut réagir très vite. Le pire serait de ne pas être préparé et que la presse apprenne quelque chose sans nous, invente ce qui se passe. Une information incorrecte est extrêmement difficile à rectifier ensuite.

Côté communication interne, la première décision a été de maintenir la confidentialité. On a essayé de limiter au maximum le nombre de personnes impliquées, et tous les employés ou fournisseurs qui ont travaillé sur le dossier ont resigué un accord de confidentialité — c'est davantage psychologique que contractuel, puisqu'en tant qu'employé on y est déjà soumis, mais ça conscientise les personnes concernées.

Et quand arrive le moment de la première communication externe, on synchronise impérativement la communication externe et interne : vos employés ne doivent pas apprendre par la presse ce que vous n'avez pas encore dit en interne. Cette synchronisation est extrêmement importante.

Interviewer : *Quelles ont été les réactions du grand public et des médias suite à cette fuite ?*

Interviewé(e) : Forcément, les médias réagissent très rapidement dans ce type de dossier — on a eu droit aux gros titres pendant quelques jours. Mais ça n'a pas duré : il y a eu des communications pendant une dizaine de jours environ, avec un impact finalement assez limité. En fait, les fuites de données sont tellement fréquentes — pratiquement toutes les semaines dans de grandes organisations, en France, en Belgique — que ça ne crée plus autant de bruit qu'on pourrait le croire.

Je fais une grande distinction entre le marché résidentiel et le marché entreprise.

Sur le marché résidentiel, c'est-à-dire le grand public, les gens en ont parlé un peu, et puis avec la fin des vacances et la rentrée, plus personne n'en parlait.

Sur le marché entreprise, en revanche, c'est beaucoup plus compliqué. On a été relancé plusieurs fois. Il y a eu des communications individuelles vers les grands comptes — des sociétés d'État comme la SNCB, des organisations militaires, l'OTAN, mais aussi de grands clients industriels comme TotalEnergies. Le patron d'Orange a rencontré personnellement les dirigeants de ces organisations pour expliquer ce qui s'était passé, rassurer sur ce qui les concernait directement, et bien leur faire comprendre qu'il n'y avait pas eu d'impact sur leurs données. Ces rencontres se sont étalées sur trois à quatre mois.

Ce qu'il faut comprendre aujourd'hui, c'est que l'image est souvent plus impactée que les données elles-mêmes. Les données qui ont fuité dans notre cas — des adresses e-mail,

des informations qui avaient déjà été compromises 25 fois ailleurs — avaient un impact réel limité. Mais l'image de l'entreprise, elle, souffre.

Interviewer : *Dans quel délai une organisation doit-elle communiquer publiquement après la découverte d'une fuite de données ? Faut-il attendre d'avoir toutes les informations ou prendre la parole rapidement quitte à y revenir ensuite ?*

Interviewé(e) : Non, il ne faut pas attendre. C'est aussi quelque chose qu'il faut gérer avec une extrême attention. Vous avez une obligation légale de communiquer le plus vite possible — d'abord aux autorités de protection des données, ensuite vers le monde extérieur.

Cela dit, au moment où vous contactez la DPA, vous pouvez leur expliquer que vous n'êtes pas encore prêt à communiquer publiquement, et leur présenter votre plan d'investigation et votre calendrier. Parce qu'il faut s'assurer de communiquer l'ensemble de l'information d'un coup et éviter les communications en série qui génèrent plus de confusion que de clarté.

Un des points sur lesquels nous avons été extrêmement vigilants, c'est le nombre exact de clients impactés. Au début, les chiffres variaient au fur et à mesure des analyses — on pensait qu'il y en avait tant, puis l'analyse révélait que c'était différent. C'est crucial de bien gérer ça avant de communiquer publiquement.

Il y a donc trois risques principaux à gérer : l'opérationnel, le réputationnel, et le financier — car vous pouvez recevoir des amendes de la part des autorités de protection des données. Dans notre cas, nous sommes encore aujourd'hui en cours d'audit par cette autorité, qui instruit le dossier pour déterminer si une amende doit être prononcée.

Interviewer : *Quel contenu et quel ton Orange a-t-il adopté dans ses communications officielles après la fuite de données ?*

Interviewé(e) : Être le plus transparent, le plus complet et le plus rapide possible. Ces trois principes résument notre approche : transparent, complet, rapide. Il n'y a aucun intérêt à traîner ou à manquer de transparence dans ces situations-là.

Interviewer : *Quels canaux de communication avez-vous utilisés lors de cette fuite de données ?*

Interviewé(e) : Pour la communication avec les autorités, c'est une communication directe via des points de contact dédiés — en Belgique, il y a deux contacts principaux au niveau de l'État.

Pour la presse, il y a deux approches. L'approche informelle : appeler directement un journaliste de confiance pour donner de l'information en avance, comme je le mentionnais. Et l'approche officielle : rédiger une communication formelle avec un numéro de téléphone pour les journalistes souhaitant plus d'informations, ou un communiqué de presse. Dans notre cas, c'est principalement via communiqué de presse que nous avons communiqué.

Interviewer : *Au-delà de la communication immédiate, quelles actions concrètes Orange a-t-il mises en place suite à cet incident ? Quelles leçons en avez-vous tirées ?*

Interviewé(e) : L'impact en interne a été considérable. On a changé l'organisation : on a renforcé le département sécurité au sens large, regroupé des personnes qui travaillaient dans des équipes séparées. On a alloué un budget supplémentaire pour lancer des projets structurels de long terme, et d'autres interventions à très court terme.

Dès les premières heures suivant la découverte du système compromis, nous l'avons mis à l'arrêt.

L'impact réputationnel externe a finalement été limité. En revanche, en interne, ça a été une sorte d'électrochoc. Ça a permis de dire : dans ce domaine, ça vaut vraiment la peine d'investir. On avait déjà eu certaines alertes, et cet incident a servi d'accélérateur.

Sur l'organisation de la gestion de crise, la grande leçon c'est d'avoir absolument deux cellules indépendantes : une cellule technique, qui gère l'incident, et une cellule de gestion de crise et de communication. La première crise, on s'est rendu compte que la cellule technique — naturellement très mobilisée sur la résolution — mettait moins de focus sur la gestion de crise et la communication. Il faut deux entités indépendantes, avec deux managers indépendants, coiffées par un grand manager qui fait le lien.

Troisième point : il faut s'y préparer en amont, y compris techniquement. Investir dans les solutions de sécurité, certes, mais surtout dans la formation et la sensibilisation des équipes — parce qu'une grande partie de la problématique est humaine. Dans notre cas, la cause initiale de l'incident était principalement humaine.

Entretien 3 — Carole Schwartz

Responsable Marketing et Communication, Membre de la direction d'une banque luxembourgeoise

Interviewer : *Pouvez-vous me présenter votre parcours et votre rôle actuel ?*

Interviewé(e) : J'ai terminé mes études à Louvain-la-Neuve en 2003 en relations publiques. Après quelques petits emplois et une insertion professionnelle au Luxembourg en tant que chargée de communication, j'y suis restée pendant 20 ans, occupant différents rôles en communication, marketing et relations publiques, avant de terminer au niveau de la direction communication et marketing. J'ai ensuite eu une opportunité au sein d'une banque, où je suis aujourd'hui cheffe du département marketing.

Interviewer : *Êtes-vous régulièrement confrontée à des problématiques de communication de crise ou de sécurité des données ?*

Interviewé(e) : Oui, de plus en plus. On y est confronté directement : via les médias, via les concurrents, mais aussi via l'évolution du digital et du phishing en général. Il faut rester de plus en plus vigilant. Et il y a aussi notre régulateur — la CSSF — qui veille et auprès de qui il faut régulièrement montrer patte blanche sur certains sujets.

Interviewer : *Comment votre organisation perçoit-elle aujourd'hui le risque d'une fuite de données ? Est-ce un sujet qui a pris de l'importance ces dernières années ?*

Interviewé(e) : Je pense que les fuites de données ont toujours existé. Ce qui a changé, ce sont les moyens utilisés, et la réponse que l'on apporte : aujourd'hui, on essaie d'être préventif plutôt que réactif. On met des outils en place en amont pour contrecarrer les fuites potentielles. Ce n'est pas toujours évident, car ces fraudes se réinventent constamment et certaines choses nous surprennent. Mais oui, il faut évoluer, rebondir, agir et rester en alerte en permanence.

Interviewer : *Y a-t-il eu des incidents récents dans le secteur qui ont changé la manière dont vous abordez ce risque ?*

Interviewé(e) : Dans le secteur bancaire, il y a beaucoup de choses : des conseillers fictifs, des brochures reproduites à l'identique imitant celles de l'entreprise, des sites web frauduleux. Tout cela dans le seul but de récupérer les identifiants de connexion des clients. Il faut bien savoir qu'aucune banque ne demandera jamais ses identifiants à un client — ni par e-mail, ni par téléphone, ni par aucun autre moyen. C'est d'ailleurs l'objet d'une grande campagne de sensibilisation menée l'an dernier au Luxembourg. Malheureusement, nombreux sont ceux qui continuent à les donner.

D'autres dispositifs ont été mis en place, comme le système VOP — Verification of Payee — qui permet de s'assurer que le paiement est bien effectué à la bonne personne grâce à un système de correspondance. C'est désormais réglementé et obligatoire.

Interviewer : *En quoi une fuite de données constitue-t-elle une crise particulière pour une organisation ? Quels sont les impacts les plus significatifs sur la réputation et la confiance ?*

Interviewé(e) : Un manque de confiance immédiat, la peur chez les clients, des retraits d'argent, des départs vers les concurrents parce qu'on ne se sent plus en sécurité. La sécurité et la confiance, c'est vraiment le plus important dans notre milieu. Et une fuite de données peut créer un effet boule de neige considérable : au Luxembourg, tout va très vite. La communication s'enchaîne, tout le monde parle, les choses s'emballent, et les conséquences peuvent être dramatiques.

Interviewer : *Avez-vous été confrontée à une fuite de données dans votre organisation ou dans une avec laquelle vous avez collaboré ?*

Interviewé(e) : Personnellement non. Je sais que dans l'organisation où je travaillais auparavant, il y en a eu une, mais ça n'a jamais été rendu vraiment public — on a essayé de gérer ça discrètement.

Interviewer : *Quel cas de gestion de crise — réussi ou raté — vous a le plus marquée ?*

Interviewé(e) : Nous faisons régulièrement des tests de gestion de crise. Nous avons une cellule de crise opérationnelle, avec tous les moyens nécessaires : nos téléphones sonnent à l'improviste, on se retrouve tous dans la cellule, et il faut réagir. C'est toujours bien préparé.

Cela dit, je pense que si ce n'était pas préparé, on ne serait pas là où on en est. Parce qu'en vraie situation, ça ne se passe pas comme ça. Il faut un plan de crise écrit, une cellule de crise clairement identifiée, avec des réponses aux questions : qui contacter, quand, comment, par quel canal, et que faire si certains canaux ne fonctionnent plus ?

C'est comme les exercices d'évacuation à l'école : en simulation, tout le monde sort dans le calme et la tranquillité. Le vrai jour, ce sera différent.

Je n'ai pas eu de vraie crise avérée à gérer moi-même, mais la théorie est là. En tout cas, je pense que face au public, il faut être transparent et prendre la parole rapidement. Il faut aussi centraliser la communication sur une seule personne clairement identifiée et s'assurer que les autres, ceux qui ne sont pas au courant de tous les détails, ne prennent pas la parole.

Interviewer : *À quel moment et dans quel délai une organisation devrait-elle communiquer publiquement après la découverte d'une fuite de données ? Faut-il tout savoir avant de parler, ou vaut-il mieux prendre la parole rapidement ?*

Interviewé(e) : Il faut prendre la parole rapidement et rassurer. C'est la base, même sans tout savoir. Il ne faut pas trop s'avancer — car il y a des éléments qu'on ne maîtrise pas encore : l'étendue des données concernées, les clients potentiellement touchés. Mais ne pas communiquer, c'est une erreur. La non-communication est, à mon sens, la pire des stratégies.

Interviewer : *Qui décide du moment de la communication publique dans votre organisation ?*

Interviewé(e) : C'est la cellule de crise. Au sein de notre département marketing et communication, deux personnes en font partie, dont moi. Les décisions se prennent avec le comité de direction, qui y participe de manière intégrante. Ce sont d'ailleurs eux qui ont la légitimité pour prendre la parole publiquement.

La cellule de crise chez nous réunit le comité de direction, le responsable banque commerciale, le risk management, la communication, et selon les cas, des suppléants spécialisés : crédit, paiements, IT, etc.

Interviewer : *Que pensez-vous de la stratégie consistant à révéler soi-même la fuite avant que les médias ou des tiers ne le fassent ? Quels en sont les avantages et les risques ?*

Interviewé(e) : L'avantage principal, c'est de ne pas laisser les médias parler de quelque chose qu'ils ne maîtrisent pas. Le risque, c'est de mettre tout le monde en état d'alerte pour un incident qui, finalement, n'était peut-être pas si grave.

C'est pour ça qu'il faut rapidement se réunir, évaluer la situation, identifier les failles et comprendre l'étendue réelle du problème.

Nous avons par exemple un contrat cadre avec une agence de communication et de presse, disponible en temps de crise en très peu de temps. Des communiqués de presse sont déjà préparés pour certains scénarios prédéfinis, afin de pouvoir les envoyer immédiatement. Car aujourd'hui, la presse ne rédige généralement plus elle-même : elle reçoit un communiqué et s'en inspire pour rédiger son article. Il faut donc être rapide pour envoyer ce communiqué.

Interviewer : *Quel contenu et quel ton une organisation devrait-elle adopter dans ses communications officielles après une fuite de données ? Comment trouver le bon équilibre entre reconnaître sa responsabilité et protéger ses intérêts juridiques ?*

Interviewé(e) : Il faut avant tout rassurer. La panique est mauvaise conseillère, et les coûts d'une panique collective sont bien plus élevés que ceux d'une communication bien maîtrisée. Il faut d'abord rassurer en interne : si les employés ne sont pas rassurés, ils ne pourront pas rassurer leurs clients à leur tour.

Nous avons mis en place l'an dernier un fichier Excel structuré — un arbre décisionnel — qui précise, en fonction du type de crise, qui alerter en premier, comment, quel ton adopter. Est-ce qu'on rassure ? Est-ce qu'on est confiant ? Est-ce qu'on désamorce ? En parallèle, des communiqués rédigés à l'avance dans les trois langues, avec l'agence, sont disponibles immédiatement.

Ce même dispositif est encadré par notre régulateur. En tant que banque coopérative, notre interlocuteur est la CSSF. On a des comités risques réguliers — risque opérationnel, risque IT, risque de résolution, risque crédit — et le nombre de sous-comités a explosé ces dernières années.

Interviewer : *Y a-t-il des formulations ou des postures à éviter absolument ?*

Interviewé(e) : S'excuser, je dirais. On peut être transparent, on assume, mais je ne pense pas qu'il faille s'avilir. Il faut rester transparent et digne.

Regardez ce qui se passe sur les réseaux sociaux : des entreprises se font démonter, et que font-elles ? Elles suppriment les commentaires négatifs, elles n'assument pas. C'est exactement ce qu'il ne faut pas faire. Il vaut mieux laisser les messages et y répondre de manière transparente, en assumant la responsabilité — sans pour autant afficher de la faiblesse. Il faut montrer qu'on est là, qu'on gère. Pas de "c'est catastrophique, on est vraiment désolé" qui donnerait l'impression qu'on a perdu le contrôle.

Surtout dans des secteurs aussi sensibles que la banque ou l'assurance : on parle de l'argent des gens, de leur investissement, de leur portefeuille.

Interviewer : *Quels canaux de communication privilégiez-vous pour informer le grand public lors d'une fuite de données ? Le choix du canal influence-t-il la manière dont le message est reçu ?*

Interviewé(e) : Ça dépend vraiment de l'audience. Il y a des clients qui iront sur notre site internet — il faut donc y avoir un message visible. Il y a les réseaux sociaux, qui permettent une diffusion très rapide si on veut toucher tout le monde. Et il y a le communiqué de presse, dont l'impact dépend aussi du timing : si la crise survient un samedi, l'utilité d'un communiqué envoyé ce jour-là est plus limitée.

Prenons un exemple concret : l'an dernier, il y a eu un problème avec les terminaux de paiement. Tout le monde donnait la faute aux banques, alors que les cartes sont gérées par les prestataires de paiement. Nous avons immédiatement mis un message sur les

réseaux sociaux pour informer nos clients de la situation et les rassurer. C'est le canal le plus rapide dans ce type de cas.

Interviewer : *Les réseaux sociaux sont-ils selon vous une opportunité ou un risque supplémentaire en situation de crise ?*

Interviewé(e) : Je pense que les réseaux sociaux attirent plutôt du négatif, mais ça dépend du public qui interagit. Dans notre cas, les abonnés d'une banque ne sont généralement pas les jeunes les plus actifs sur ces plateformes. Cela dit, chaque réseau a sa population, et chaque réseau nécessite un ton et un texte adaptés — LinkedIn n'est pas Facebook, et Facebook n'est pas Instagram. Il faut les utiliser, mais intelligemment.

Interviewer : *Au-delà de la communication immédiate, quelles actions concrètes une organisation devrait-elle mettre en place pour démontrer qu'elle a tiré les leçons de l'incident et pour reconstruire la confiance ?*

Interviewé(e) : Il faut analyser les failles : pourquoi c'est arrivé, comment y remédier, quels outils mettre en place au niveau IT. Chez nous, suite à l'apparition de sites frauduleux imitant notre plateforme internet banking, nous avons adopté un outil de veille — Netcraft — qui détecte en temps réel les sites usurpant notre identité ou notre nom, et nous remonte des alertes directement. Il y a plein d'initiatives comme ça.

Mais je pense que l'avenir nous demandera encore plus d'investissements dans la sécurité. Et malgré tout, les gens continuent à partager leurs identifiants — pas seulement les personnes âgées, on a aussi des jeunes qui se font pirater, de façon surprenante. Les faux sites sont de plus en plus convaincants, il est de plus en plus difficile de les distinguer des vrais.

Interviewer : *Votre organisation dispose-t-elle d'un plan de communication spécifique prévu pour les fuites de données ou cyberattaques ? Si oui, comment est-il structuré et qui implique-t-il ?*

Interviewé(e) : Oui, c'est précisément l'arbre décisionnel dont je parlais. Tout y est noté : selon telle situation, voilà ce qu'on fait. C'est révisé chaque année — ce sont des procédures et des politiques internes qui ont des échéances de révision formelles. On vérifie ce qui est à jour, ce qui doit être adapté, quelles personnes doivent être informées — conseil d'administration, comité de direction, partenaires selon les cas.

Interviewer : *Si vous deviez conseiller une organisation qui vient de découvrir une fuite de données significative, quelles seraient vos trois recommandations prioritaires en matière de communication ?*

Interviewé(e) : Premièrement, communiquer rapidement, avec des mots simples et rassurants.

Deuxièmement, assumer. Reconnaître qu'il y a eu une fuite, expliquer que la situation est maîtrisée, que des mesures ont été prises pour que ça ne s'étende pas davantage. Sans s'excuser de manière excessive, mais en étant transparent sur ce qui s'est passé.

Troisièmement, agir concrètement pour les personnes touchées. Si des clients ont été impactés, les contacter directement via leur conseiller, leur offrir un suivi personnalisé. Ça dépend évidemment de l'ampleur de l'incident et de la taille de l'organisation.

Interviewer : *À l'inverse, quelles sont les erreurs les plus fréquentes et les plus coûteuses à éviter ?*

Interviewé(e) : Ne rien dire. Rejeter la faute sur les autres. Et ne pas mettre en place des mesures correctives après l'incident.

Faire l'autruche, ce n'est pas une stratégie. Il faut communiquer — via le bon canal, avec le bon ton — et surtout éviter le jargon technique. Des mots simples, un message

rassurant. Si vous êtes trop technique ou trop compliqué, vous perdez les gens au lieu de les rassurer.

En résumé : rapidité, transparence, assumer — et des mots simples.

Entretien 4 — Stephanie Tosato

Head of Corporate Communication dans une banque luxembourgeoise

Interviewer : *Pouvez-vous me présenter votre parcours et votre rôle actuel ?*

Interviewé(e) : Cela fait 20 ans que je travaille en communication et marketing. La première partie de ma carrière s'est déroulée plutôt côté marketing, pour des sociétés internationales — satellites, fonds d'investissement, identité numérique, etc. Depuis cinq ans, je suis dans le monde de la communication corporate, en rejoignant la banque actuelle.

Interviewer : *Êtes-vous régulièrement confrontée à des problématiques de communication de crise ou de sécurité des données ?*

Interviewé(e) : Communication de crise, oui. Sécurité des données, un peu moins directement. Les domaines sur lesquels on intervient en communication corporate, c'est tout ce qui peut impacter la réputation de l'entreprise — un client insatisfait, une problématique interne, un sujet particulier. Les sujets de sécurité arrivent de plus en plus souvent, mais surtout sous l'angle de la fraude. Je n'ai jamais eu à faire face à une véritable fuite de données que j'aurais dû adresser au niveau du grand public.

Interviewer : *Comment votre organisation perçoit-elle aujourd'hui le risque d'une fuite de données ?*

Interviewé(e) : Complètement, et d'autant plus avec la nouvelle réglementation DORA, qui nous demande d'être extrêmement résilients sur le sujet. En tant que banque systémique, nous avons de plus en plus d'obligations venant de l'Union européenne sur notre préparation en cas de problème. L'Union européenne teste régulièrement la résilience des entreprises systémiques pour s'assurer qu'en cas d'incident, un plan de communication peut être déployé très rapidement. Il faut donc avoir des plans de crise testés régulièrement.

Interviewer : *Y a-t-il eu des incidents récents dans votre secteur qui ont changé la manière dont vous abordez ce risque ?*

Interviewé(e) : Il y a deux éléments qui ont changé notre perception. Premièrement, les réseaux sociaux : la diffusion de l'information est beaucoup plus rapide, et pour une banque, ça peut prendre une dimension critique — les gens paniquent et viennent retirer leur argent. C'est ce qui s'est passé avec la Silicon Valley Bank, et les crises bancaires de 2008 ont également intégré cette dimension.

Deuxièmement, les cyberattaques récentes au Luxembourg sur des prestataires comme la Poste ont renforcé notre vigilance. Si un centre de données ou un accès internet tombe, ça nous impacte directement. Et le contexte géopolitique actuel augmente le risque d'attaques ciblées sur des organisations systémiques.

Interviewer : *En quoi une fuite de données constitue-t-elle une crise particulière pour votre organisation ?*

Interviewé(e) : La confiance, très clairement. On gère des informations sensibles : coordonnées personnelles, numéros de compte, données financières — la vie privée des gens, en somme. Tout dépend de la nature de la fuite. Une fuite sur les données

d'employés, c'est déjà un incident sérieux. Mais une fuite sur des données clients, c'est bien plus grave.

L'ampleur est aussi déterminante : on ne réagit pas de la même façon si deux e-mails ont été envoyés par erreur à la mauvaise personne, ou si tous les dossiers clients avec leurs numéros de carte bancaire ont été exposés. L'ampleur de la crise dépend de l'ampleur de la fuite et des types de données concernées.

Est-ce que la cause — négligence interne ou attaque externe — change la perception du public ? Pas vraiment. Ce qui compte, c'est l'ampleur de la fuite et les conséquences pour les personnes concernées.

Interviewer : *Avez-vous déjà été confrontée à une fuite de données dans votre organisation ?*

Interviewé(e) : Il peut y avoir des choses plus restreintes, comme un e-mail envoyé à la mauvaise personne. On n'a jamais eu à communiquer au grand public. Il faut savoir qu'en cas de fuite avérée, on a 72 heures pour la signaler à la CNPD, et selon l'ampleur, une obligation de communiquer aux clients ou au grand public. Tant mieux, on touche du bois.

Interviewer : *Imaginons une fuite de données dans votre organisation. Dans les grandes lignes, comment le plan de communication s'appliquerait-il ?*

Interviewé(e) : Une fuite de données s'inscrit dans le schéma des communications de crise. Quand on identifie une problématique, elle doit être signalée aux membres du comité de direction. Si on établit qu'il s'agit effectivement d'une crise avec un impact réputationnel potentiel, on commence à déployer le plan de crise.

Si c'est une crise majeure, un groupe défini au sein de la banque est convoqué en urgence via une alerte téléphonique — même les congés ne sont pas une excuse — et on se réunit en ligne. On reçoit les premières informations sur la situation et son ampleur, et on définit les actions.

On décide d'abord des actions de remédiation : blocage d'accès, arrêt de certains systèmes, etc. En parallèle, on prépare un communiqué pour la presse. On détermine ce qu'on dit aux employés, comment circule l'information, quelles sont les conséquences sur l'activité quotidienne. On définit également ce qu'on dit aux clients et comment on le fait : réseaux sociaux, messagerie sécurisée, bannière sur le site, etc. Et on détermine si le dirigeant doit prendre la parole publiquement.

Interviewer : *À quel moment et dans quel délai une organisation devrait-elle communiquer publiquement après une fuite de données ?*

Interviewé(e) : Le plus rapidement possible — à partir du moment où on est suffisamment informé pour comprendre la situation. Le danger d'une information partielle, c'est de risquer de créer la panique, avec un risque réputationnel énorme. Il faut trouver le bon équilibre : communiquer trop vite sans avoir les informations peut aussi poser un problème de confiance. C'est un peu comme en médecine : il faut peser le bénéfice. Est-ce que ne pas communiquer tout de suite a un impact sur la sécurité de nos clients ? Si oui, il faut les informer sans attendre pour qu'ils puissent prendre les actions nécessaires pour se protéger.

Interviewer : *Qui décide du moment de la communication dans votre organisation ?*

Interviewé(e) : La communication de crise est proposée par l'équipe com, mais si c'est une crise majeure, elle doit être vue et validée par les membres du comité exécutif, et même par le conseil d'administration — parce qu'on engage la responsabilité de l'entreprise.

Interviewer : *Quel contenu et quel ton une organisation devrait-elle adopter dans ses communications officielles après une fuite de données ?*

Interviewé(e) : Informatif, pédagogique, et en langage simple. Ce qu'on veut éviter absolument, c'est le jargon. Toute personne concernée doit pouvoir comprendre ce qui s'est passé, ce que ça signifie pour elle, et si elle a une action à entreprendre. On évite le vocabulaire corporate compliqué. En résumé : qu'est-ce qui s'est passé ? Qu'est-ce que ça signifie pour vous ? Y a-t-il quelque chose à faire de votre côté ? Quelles actions avons-nous mises en place ?

Interviewer : *Y a-t-il d'autres formulations ou postures à éviter absolument ?*

Interviewé(e) : La panique. Si vous-même semblez stressé ou paniqué dans votre communication, vous n'inspirez pas confiance. Il faut montrer que vous maîtrisez la situation. Éviter également de s'avancer : si les informations ne sont pas toutes disponibles et que la communication doit se faire rapidement, on dit ce qu'on sait — pas ce qu'on suppose. Spéculer est interdit : vous risquez d'induire les gens en erreur, et ça peut vous être reproché par la suite. Si vous dites "il n'y a pas eu de fuite" et qu'en fait il y en avait une, vous aurez le retour de bâton. Il faut donc rester calme, établir un processus clair : voilà ce qu'on sait, voilà ce qu'on a fait, voilà ce qu'on va faire.

Interviewer : *Quels canaux de communication privilégiez-vous pour informer le public lors d'une fuite de données ?*

Interviewé(e) : On part toujours du cercle privé vers l'extérieur. D'abord les personnes en interne, puis les clients, puis la presse. Il n'y a rien de pire qu'un employé qui apprend quelque chose par la presse. Pour les clients, on utilise la messagerie sécurisée, une bannière sur le site, et des appels téléphoniques pour les clients les plus proches — grands comptes, relations managers. Pour le grand public, le communiqué de presse. Nous intégrons aussi désormais les push notifications via l'application mobile comme canal complémentaire — c'est très efficace pour toucher directement nos clients.

Interviewer : *Les réseaux sociaux sont-ils une opportunité ou un risque en situation de crise ?*

Interviewé(e) : Plutôt une opportunité si on les utilise bien. L'avantage, c'est qu'on peut prendre l'initiative de communiquer plutôt que de subir une vague d'informations non maîtrisées. Ça nous permet de répondre directement aux clients qui s'inquiètent. Bien sûr, ça entraîne des commentaires parfois désobligeants. Mais si on communique sur les réseaux sociaux, on a plus de probabilité d'être vu et partagé qu'avec une messagerie sécurisée que tout le monde ne consulte pas tous les jours.

Interviewer : *Au-delà de la communication immédiate, quelles actions concrètes une organisation devrait-elle mettre en place pour reconstruire la confiance après une fuite de données ?*

Interviewé(e) : Je ne suis pas experte en cybersécurité, mais de mon point de vue : si on met en place des actions qui auraient dû être des mesures de base et qu'on ne les avait pas encore, les communiquer après coup peut être perçu comme un aveu de lacune. En revanche, dans le contexte actuel — avec l'IA, les agents intelligents et des solutions informatiques de plus en plus sophistiquées —, des mises à jour régulières sont légitimes.

La confiance se construit sur des années. On dit souvent que vous mettez dix ans à la construire et dix secondes à la détruire. Ce n'est pas par un grand plan de communication qu'elle se reconstruit, mais par des actions concrètes et incrementales, au fil du temps — et les gens s'en rendent compte.

Interviewer : *Si vous deviez conseiller une organisation qui vient de découvrir une fuite de données, quelles seraient vos trois recommandations prioritaires ?*

Interviewé(e) : Premièrement, comprendre. Prenez le temps d'écouter, de poser les bonnes questions, de bien mesurer les implications. Il y a beaucoup de choses à cerner avant d'agir.

Deuxièmement, coordonner. Établir rapidement un plan de communication, avec toutes les bonnes personnes autour de la table pour prendre des décisions rapides et coordonnées. Rien de pire que de passer quatre heures à se demander qui fait quoi.

Troisièmement, monitorer. La situation évolue et votre message doit s'adapter en fonction des nouvelles informations et des réactions. Et idéalement, avant tout ça : se préparer en amont.

Interviewer : *Selon vous, existe-t-il une bonne pratique qui se démarque dans la gestion d'une crise cyber, que vous ayez observée dans votre organisation ou ailleurs ?*

Interviewé(e) : Pour moi, la meilleure pratique, c'est de rassembler les bonnes personnes le plus vite possible. Plus une entreprise est grande, plus c'est important d'avoir identifié à l'avance qui doit être autour de la table, avec des remplaçants identifiés en cas d'absence.

Et dans les cas que j'ai observés, ce qui fonctionne le mieux, c'est une communication externe simple, sans chercher à cacher les choses, claire et transparente. Quand on fait face à une fuite de données, l'audience est composée de personnes de tous horizons. La bonne pratique, c'est de parler de façon à ce que tout le monde comprenne. Les communications les plus simples, les plus humaines et les plus transparentes sont celles qui ont le maximum d'impact.

Entretien 5 — Pascale Kauffman

CEO d'une société de conseil indépendante spécialisée dans la communication stratégique, la communication de crise, les relations médias, la gestion de la réputation et les affaires publiques et gouvernementales

Interviewer : *Pouvez-vous me présenter votre parcours et votre rôle actuel ?*

Interviewé(e) : J'ai fait des études en sciences de la communication et en relations publiques à l'Université libre de Bruxelles, avec un Master en journalisme et communication, spécialisation relations publiques. Après un stage en journalisme et un passage en agence de communication, je suis revenue au Luxembourg et j'ai commencé dans la communication institutionnelle d'Astra — le plus grand opérateur de satellite au monde à l'époque, entreprise luxembourgeoise basée à Betzdorf. J'y ai travaillé pendant 12 ans dans différentes missions, d'abord en communication et marketing, puis en tant que directrice pour l'Italie et responsable du sud de l'Europe.

En 2007, j'ai rejoint la Ville de Luxembourg comme directrice de la communication — un travail très différent, qui couvre tous les aspects de la communication : porte-parole, discours, gestion de l'actualité quotidienne et des crises. J'y ai observé un manque de pensée stratégique dans la communication publique, ce qui m'a amenée, cinq ans plus tard, à fonder ma propre société de conseil en communication stratégique et gestion de crise. Elle existe depuis maintenant 14 ans et s'appelle Apollo Strategies — un nom inspiré de la mission Apollo, symbole pour nous d'un vecteur pour les organisations vers une contribution proactive à l'économie luxembourgeoise.

Je suis également membre de plusieurs conseils d'administration, notamment de Loxenberg et du groupe médias luxembourgeois.

Interviewer : *Comment percevez-vous le risque d'une fuite de données pour les organisations que vous accompagnez ?*

Interviewé(e) : Il est imminent. Une organisation qui pense aujourd'hui qu'une fuite de données n'est pas possible se trompe. Cela dit, la fuite de données n'est qu'un aspect d'une cyberattaque. On n'a pas toujours une fuite de données : ça dépend de la santé informatique de l'organisation et de sa préparation. Comme le disent nos amis IT : la question n'est pas de savoir si on sera attaqué un jour, mais quand. Il faut donc être préparé. Et la fuite de données ne résulte pas systématiquement d'une cyberattaque — ça dépend vraiment de chaque situation.

Interviewer : *En quoi une fuite de données constitue-t-elle une crise particulière pour une organisation ?*

Interviewé(e) : Sur la confiance, d'abord — c'est l'aspect le plus important. Quand des données personnelles sont exposées ou rendues publiques, la confiance est évidemment détruite. Au Luxembourg, qui est une grande place financière, si un acteur financier perd des données, les conséquences sont considérables.

On a d'ailleurs vu des situations paradoxales : des clients qui ouvraient leur espace bancaire et voyaient le compte de quelqu'un d'autre. Ce sont des moments extrêmement inconfortables pour tout le monde — l'utilisateur n'a pas le droit de regarder ces données, même si on les lui montre par erreur.

Tout dépend aussi de la rapidité de réaction de l'organisation. Dans une crise où vous tardez à répondre à vos parties prenantes, la confiance se dégrade de façon dramatique.

Interviewer : *Avez-vous déjà été confrontée à une fuite de données dans votre organisation ou dans une organisation avec laquelle vous avez collaboré ?*

Interviewé(e) : Nous sommes gestionnaires de crise — on vient nous chercher pour préparer, et on vient nous chercher aussi en urgence. Au sein de notre structure, nous n'avons pas encore subi d'incident majeur, même si nous recevons des attaques de phishing régulièrement et que notre prestataire informatique nous informe des tentatives en cours.

Le Luxembourg est particulièrement ciblé dans le Darknet. Mais en tant que gestionnaires de crise, nous sommes très souvent sollicités par des organisations qui traversent ce type de situation — dans tous les secteurs, y compris des prestataires de taille importante.

Interviewer : *Lorsque vous collaborez avec une entreprise qui a subi une fuite de données, quelles sont les règles d'or à suivre pour bien communiquer ?*

Interviewé(e) : La première règle, c'est de se préparer en amont. Il faut un plan de continuité d'activité qui intègre un plan de gestion de crise, lui-même incluant un plan de communication de crise. Ces trois éléments doivent être cohérents entre eux : si le plan de communication a des niveaux d'urgence différents de ceux du plan de continuité, vous aurez une crise dans la crise.

Il faut que les personnes clés connaissent ce plan, y aient contribué, et qu'il soit révisé au moins deux fois par an. Des simulations régulières sont indispensables. La communication interne sur ce plan est extrêmement importante.

Nous travaillons avec trois étapes : la préparation, l'action dans le feu de la crise, et la reconstruction de la confiance après.

Dans le feu de l'action, on nous appelle souvent comme pompiers. La première réaction d'une organisation est souvent de communiquer vers l'extérieur — or, la communication interne est la première priorité. Il faut aussi analyser la situation avant de parler, sans pour autant attendre trop longtemps.

Je me souviens d'un grand acteur luxembourgeois qui a affirmé que ses services n'étaient pas disponibles mais que ce n'était pas une cyberattaque — pour se rendre

compte ensuite que c'en était bien une. C'est la pire erreur qu'on puisse faire : affirmer quelque chose qu'on ne sait pas encore avec certitude.

Chaque minute compte dans une crise. Il faut commencer par communiquer en interne, puis s'adresser aux parties prenantes externes, en respectant un ordre de priorité : d'abord la CNPD si on a une cyberattaque, le ministère responsable, éventuellement un ministre de tutelle — même si la communication n'est pas encore publique. Avec les médias, on peut gérer de façon réactive au début si on n'a pas toutes les informations. Si vous êtes fournisseur de services au grand public — comme un opérateur de télécoms — les clients se rendront compte très vite qu'il y a un problème : il faut les rassurer rapidement, en leur indiquant ce qu'on est en train de vérifier et quand on reviendra vers eux.

Interviewer : *Dans quel délai une organisation devrait-elle communiquer publiquement après une cyberattaque ? Le délai de 72 heures imposé par le RGPD vous semble-t-il réaliste ?*

Interviewé(e) : 72 heures, c'est parfois très long — et parfois très court. Ça dépend vraiment de la situation. Si la cyberattaque survient un week-end, vous n'avez souvent pas les équipes nécessaires immédiatement disponibles pour identifier les causes et l'ampleur.

Et ça dépend aussi de votre organisation : si vous faites partie des entreprises qui contribuent à la résilience d'un pays — ce que le Luxembourg est en train de formaliser dans sa stratégie de résilience nationale —, vous pouvez avoir l'obligation de communiquer aux autorités dans les deux heures suivant la découverte. Les 72 heures dépendent vraiment de la gravité de la crise et du rôle de l'organisation dans le fonctionnement de la société.

Interviewer : *Quel contenu et quel ton une organisation devrait-elle adopter dans ses communications officielles après une cyberattaque ?*

Interviewé(e) : Ce doit être un ton authentique, fidèle à la culture de l'entreprise. Et il faut absolument éviter les formulations générées par l'intelligence artificielle : on reconnaît immédiatement ces phrases lisses et standardisées qui manquent d'humanité.

S'il y a des personnes blessées ou des impacts humains importants, il faut toujours démontrer de l'empathie — envers les victimes, mais aussi envers les collaborateurs.

Même quand il n'y a que des données perdues, c'est souvent un sujet très humain et émotionnel. L'organisation doit être à l'écoute de ceux qui sont lésés. Et pour ça, il faut que le ton reflète véritablement les valeurs de l'entreprise — pas les afficher artificiellement, mais les incarner par des actions concrètes.

Si une de vos valeurs est d'être proche de vos collaborateurs, montrez-le par des actions concrètes : réunissez-les en personne si possible, envoyez une vidéo pour montrer un visage humain, puis un e-mail pour toucher tout le monde. Chaque canal a son utilité, mais le sens humain doit primer.

Interviewer : *Quels canaux de communication privilégiez-vous pour informer le public lors d'une fuite de données ?*

Interviewé(e) : Aujourd'hui, il faut considérer tous les canaux disponibles et choisir ceux qui sont adaptés à la situation. Parfois, une conférence de presse s'impose — si vous êtes fournisseur de mobilité et qu'il y a eu un accident de train, il faut montrer les visages des dirigeants et parler directement au public à travers les journalistes.

En interne, si vous disposez d'un intranet ou de la capacité à faire de courtes vidéos, c'est précieux — mais ça demande beaucoup de tenue et de leadership, car on voit le vrai visage des dirigeants. Des permanences ou des portes ouvertes peuvent aussi être un moyen de communication très puissant, mais seulement si c'est dans vos habitudes :

ouvrir les portes au lendemain d'une crise alors qu'elles sont toujours fermées, les gens seront suspicieux.

Il n'y a pas de canal meilleur qu'un autre : il faut regarder la situation, comment vous fonctionnez normalement, et adapter les outils à ce que vous êtes. L'authenticité prime.

Interviewer : *Au-delà de la communication immédiate, quelles actions concrètes une organisation devrait-elle mettre en place pour reconstruire la confiance après une fuite de données ?*

Interviewé(e) : Pour reconstruire la confiance, il faut démontrer qu'on fait mieux. Il ne faut pas hésiter à nommer ce qui n'a pas fonctionné, et à expliquer les mesures prises pour que ça ne se reproduise pas. Mais il faut aussi bien choisir le moment de cette communication positive — le faire immédiatement après la crise peut être mal perçu.

Une approche que je trouve particulièrement efficace, c'est celle d'un client avec qui nous avons travaillé et qui a décidé de partager son expérience publiquement — non pas pour se vanter, mais pour que ses confrères puissent en tirer des leçons sans avoir à subir la même crise. Nous avons organisé un webinaire en invitant toutes les parties prenantes ayant contribué à la gestion de crise : la CNPD, le ministère responsable, nos équipes de communication, leurs équipes IT. Chacun a présenté son rôle, les actions entreprises, ce qui a bien fonctionné. Le webinaire a été ouvert aux confrères du secteur, et les clients ont également été invités à y assister.

Ce type d'initiative crée un moment fort de transparence, de partage et de pédagogie. L'organisation est depuis reconnue comme une référence sur ces sujets dans son secteur.

Interviewer : *Quelles sont les erreurs les plus fréquentes et les plus coûteuses à éviter en situation de crise cyber ?*

Interviewé(e) : La première erreur — et la plus coûteuse — c'est de ne pas avoir investi dans un plan de résilience ou un plan de continuité d'activité avant la crise. Quand vous arrivez dans la crise sans plan, la confiance est déjà fragilisée, et vous repartez de zéro en pleine urgence. C'est ce qui vous coûtera le plus cher.

Ensuite, ne pas communiquer, ou communiquer de façon inadaptée, si les médias apprennent votre cyberattaque avant vous. C'est une situation très délicate. Dès lors que ça concerne le grand public, il faut communiquer — mais avec les bons interlocuteurs, dans le bon ordre.

On peut très bien avoir des contacts journalistes de confiance à qui l'on donne un accès privilégié pour qu'ils comprennent bien la situation avant de publier. On leur dit : "On vous donne l'exclusivité, mais attendez qu'on vous explique le contexte." Ça fonctionne si cette relation de confiance a été construite en amont, tout au long de l'année.

Et sur les conférences de presse : attention à ne pas les streamer directement. Des entreprises ont fait cette erreur — et ça leur a coûté très cher. Les journalistes sont là pour comprendre et interpréter. Si vous streamez directement, toute approximation est immédiatement visible par des milliers de personnes, sans filtre. J'ai vu une organisation se retrouver dans une situation catastrophique parce que ses dirigeants étaient entrés trop tôt dans la salle, avaient répondu à des questions avant le début officiel de la conférence, et étaient "morts" avant même de commencer. Tout ça avait été capté et diffusé.

Déclaration sur l'honneur, mémoires de l'École de communication, UCLouvain

Je déclare qu'il s'agit d'un travail original et personnel, que toutes les sources référencées ont été indiquées dans leur totalité et ce, quelle que soit leur provenance, et que l'utilisation des outils d'intelligence artificielle est conforme aux consignes d'utilisation publiées par la Faculté ESPO et disponible à cette adresse :

https://intranet.uclouvain.be/fr/myucl/facultes/espo/intelligence-artificielle-consignes-d-utilisation-pour-les-etudiant-es.html

Je suis conscient·e que le fait de ne pas citer une source, de ne pas la citer clairement et complètement, de ne pas annoncer dans une partie spécifique en début du mémoire l'utilisation que j'ai faite des outils d'intelligence artificielle ou de les utiliser de manière contraire à ce qui est prévu dans la note facultaire constituent des irrégularités graves au regard du Règlement des études et des examens de l'Université catholique de Louvain (Chapitre 4, section 7, article 107 à 114) au sein de l'Université. J'ai notamment pris connaissance des risques de sanctions administratives et disciplinaires encourues.

Au vu de ce qui précède, je déclare sur l'honneur ne pas avoir commis de plagiat ou toute autre forme de fraude et de n'avoir pas utilisé les outils d'intelligences artificielles en dehors de ce qui est accepté à l'UCLouvain.

Nom, Prénom : Neu Guillaume

Date : 15/08/2026

Signature de l'étudiant :

UNIVERSITÉ CATHOLIQUE DE LOUVAIN
Faculté des sciences économiques, sociales, politiques et de communication
Place Montesquieu, 4 bte L2.05.01, 1348 Louvain-la-Neuve, Belgique | **www.uclouvain.be/espo**