2. PRATIQUE DE LA COLLECTE DE DONNÉES RELATIVES AUX INCIDENTS

2.1. INTRODUCTION

Si le retour d'expérience était le moteur de la gestion de la sécurité, les données en seraient le carburant, notamment parce qu'elles alimentent l'analyse des incidents significatifs et l'analyse des risques.

Le terme « *incident significatif* » tel que défini au *chapitre 1* a été étudié pour la première fois dans le Rapport technique 2009R08 [54] « *Outils de gestion de la sécurité des tunnels* » de l'AIPCR recommandant de collecter des données au moins sur les incidents suivants :

- collision causant au moins un tué ou un blessé (exigeant une attention médicale ou une hospitalisation, même de courte durée) ;
- incendie dans un véhicule qui a commencé à brûler dans le tunnel, mais a pu en sortir sans assistance ;
- incendie dans un véhicule qui a brûlé (totalement ou partiellement) à l'intérieur du tunnel ;
- fuite ou perte de marchandises dangereuses (autorisées ou non).

Pour les tunnels avec un haut degré de permanence et de surveillance (c'est-à-dire télésurveillance et contrôle permanent), il est recommandé de recueillir des données supplémentaires pour les types d'incidents suivants (en plus des incidents significatifs décrits ci-dessus) :

- Collision avec dommages matériels uniquement (pas de tués ni de blessés) ;
- Pannes ;
- Pannes techniques des systèmes tunnel (avec ou sans fermeture imprévue du tunnel).

Ce chapitre, tout comme le rapport, est axé sur les incidents significatifs. Il considérera toutefois si nécessaire la collecte des données comme un tout (ce qui peut inclure également des incidents non significatifs).

L'objectif de ce chapitre est de mieux comprendre la façon dont les données sont recueillies, y compris les difficultés d'ordre pratique et les propositions d'amélioration.

Les observations, analyses et propositions s'adressent donc essentiellement aux exploitants de tunnels, mais concerneront aussi d'autres parties intervenant dans la collecte et le traitement des données relatives aux incidents de tunnel.

Le *chapitre 2* porte sur la collecte des données relatives aux incidents de tunnel alors que les *chapitres 3, 4 et 5* montrent ce que l'on peut obtenir de l'analyse des données : statistiques (*chapitre 3 & 4*), enseignements de l'analyse d'incidents réels (*chapitre 5*). Le *chapitre 2* ne couvre pas l'analyse des données et la diffusion de l'information en découlant auprès des parties prenantes, sauf lorsque ces aspects sont directement liés à la collecte.

2.2. ÉLÉMENTS DE CONTEXTE

Le présent chapitre s'appuie sur le retour d'expérience et les pratiques d'exploitants de tunnels du monde entier.

Dans le cadre de la préparation de ce rapport, un questionnaire portant sur la collecte des données a été élaboré et envoyé dans de nombreux pays. L'objectif de ce questionnaire était de mieux comprendre l'utilisation des « *méthodes de collecte de données* » à travers le monde s'agissant des incidents non significatifs et significatifs (questionnaire en *annexe 2*). De nombreux exploitants de tunnels y ont répondu, certains y joignant même leurs propres formulaires d'enregistrement. Ces informations pratiques ont été évaluées et ont servi de base pour la rédaction de ce chapitre.

Des pays tels que la Colombie, la France, la Grèce, le Mexique, les Pays-Bas, Singapour, l'Espagne et le Royaume-Uni ont répondu au questionnaire.

Nous avons également reçu en plus les types de documents suivants :
- Deux types de formulaires d'enregistrement pour les incidents pertinents :
  - Le premier type de formulaire est utilisé par les exploitants pour consigner les données lorsque l'incident est survenu.
  - Le deuxième type est utilisé par les exploitants de tunnels pour transmettre les informations requises à l'autorité administrative.
- Rapports européens bisannuels (de 11 pays) ;
- Rapports statistiques pluriannuels (de 4 pays).

Ces documents ont fourni un éclairage particulièrement utile sur les méthodes de collecte de données et sur la façon dont les données collectées sont utilisées dans la pratique.

2.3. LA CHAÎNE DE COLLECTE DE DONNÉES

2.3.1. Principaux objectifs/applications de la collecte de données

Les informations sur les incidents en tunnel peuvent avoir de nombreux usages. Les principaux objectifs de la collecte de données sont expliqués ci-dessous sur la base des réponses fournies par les exploitants de tunnels dans le questionnaire :

- pour l'ensemble des intervenants (exploitant du tunnel, police, pompiers, etc.), ces données sont utiles pour une analyse détaillée de l'événement qui a causé l'incident et particulièrement les mesures prises par les différents intervenants (exploitants, équipe de secours interne ou externe, équipe de maintenance, etc.). L'objectif est d'évaluer la qualité des mesures prises par les équipes (réactivité, organisation, coordination, gestion, application des procédures, etc.), la pertinence et l'exécution des procédures, le système technique utilisé et l'interaction entre ce système technique et les parties prenantes concernées (notamment l'équipe de l'exploitant du tunnel). Une première analyse interne peut être réalisée et généralement les parties concernées se coordonnent systématiquement ;
- les exploitants et/ou gestionnaires de tunnel peuvent également utiliser les données pour obtenir des statistiques sur les incidents ou l'utilisation des équipements au niveau du tunnel ;

- pour les autorités régionales ou nationales : connaissances statistiques (s'appuyant souvent sur des statistiques différentes de celles utilisées par les exploitants) et/ou élément d'entrée pour l'analyse des risques.

Ces objectifs n'ont pas le même calendrier. De manière générale, l'analyse détaillée d'un incident a lieu à court ou moyen terme. Elle conduit à des modifications mineures apportées aux procédures et équipements (les changements plus importants peuvent prendre davantage de temps). Les statistiques sont établies sur le long terme, car plusieurs années de collecte sont nécessaires pour obtenir des résultats et analyses significatifs.

Les *chapitres 3* (collisions en tunnel) et *4* (incendies en tunnel) fournissent des exemples de connaissances statistiques. Le *chapitre 5* propose des exemples d'enseignements tirés à partir de l'analyse détaillée d'incidents.

La collecte de données peut également servir d'autres fins, mais celles-ci ne sont pas abordées dans le rapport, car la sécurité des usagers du tunnel n'est pas leur objectif principal. Par exemple, certaines informations peuvent être nécessaires à des fins judiciaires (pour déterminer la responsabilité en cas de collision avec blessés) et directement collectées « *sur le terrain* » par la police ou des experts. La procédure judiciaire a généralement pour objet de déterminer la responsabilité, non pas de renforcer la sécurité.

2.3.2. Différents niveaux possibles de collecte de données

Les principaux niveaux de collecte de données sont :

- niveau local : données dont les parties prenantes locales ont besoin. Ce niveau de collecte s'applique à toutes les données que l'exploitant peut obtenir directement ou indirectement (par exemple auprès des services d'intervention d'urgence) ;
- niveau du réseau : données dont les exploitants du réseau routier ou les autorités ont besoin. Ce niveau de collecte s'applique à toutes les informations requises au niveau régional ou national (notamment par les autorités). Pour que les données au niveau du réseau soient utiles, les informations recueillies au niveau du tunnel doivent dans une certaine mesure être traitées.

Dans certains pays, il n'existe qu'une seule base de données pour l'exploitant du tunnel et l'autorité. Dans ce cas, l'exploitant et l'autorité régionale ou nationale disposent donc de données identiques.

2.3.3. Rapports fondés sur les données collectées

En fonction des objectifs et des niveaux de collectes de données, l'analyse de ces dernières peut fournir les principaux rapports suivants :

- rapport détaillé sur un incident en particulier ; ce rapport enregistre officiellement l'analyse détaillée d'un incident. L'exploitant du tunnel est généralement l'auteur de ce document ;
- rapport interne de l'exploitant du tunnel, pour ses propres besoins ou pour le gestionnaire de tunnel. Ce rapport peut par exemple porter sur la qualité de la gestion et la performance des équipes et des équipements en termes de gestion d'incidents, mais également sur le

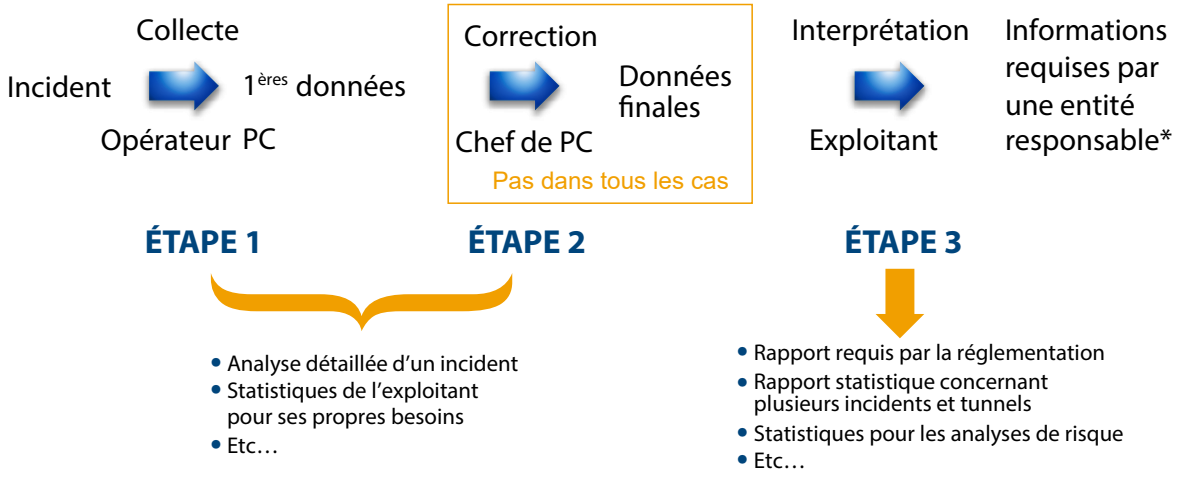
niveau de service fourni pour les usagers et les statistiques internes ;

- rapport réglementaire pour l'autorité de contrôle. Par exemple, le rapport européen bisannuel, que les États membres utilisent pour transmettre une analyse des incendies et collisions qui portent manifestement atteinte à la sécurité des usagers de la route (fréquence, causes, évaluation, rôle effectif et efficacité des installations et mesures de sécurité) à la Commission européenne en vertu de l'article 15 de la Directive 2004-54/CE du Parlement européen ;
- rapport pluriannuel (statistiques telles que les taux d'incidents) établi régulièrement par certains pays, essentiellement à des fins d'analyses statistiques : fréquence des incidents, cause, corrélation, etc.

Dans certains pays, les données collectées et les rapports qui en découlent sont confidentiels.

2.3.4. Établissement d'une chaîne de collecte de données

Comme nous venons de le voir, les données relatives aux incidents sont recueillies à diverses fins qui exigent des niveaux de collecte différents ainsi que différents sortants pour fournir un retour d'information efficace. Dans la pratique, il est possible de mettre en place une chaîne de collecte de données allant du glanage d'informations sur l'incident initial à la présentation de données relatives aux incidents aux autorités. Cette chaîne de collecte de données fait clairement intervenir le personnel d'exploitation du tunnel. La structure de base de cette chaîne de collecte de données est illustrée ci-dessous :



*(*Une entité responsable peut être le maitre d'ouvrage du tunnel, ou une autorité nationale ou locale)*

Illustration 3 : chaîne de collecte de données

Comme nous venons de le voir, la qualité du sortant et par conséquent la qualité des enseignements tirés à partir du retour d'expérience dépendent fortement de la collecte des données et bien sûr du fonctionnement de la chaîne de collecte de données. Il est donc très utile d'examiner le fonctionnement de la chaîne de collecte de données dans la pratique ainsi que d'envisager les moyens de l'améliorer.

La chaîne de collecte de données illustrée dans l'*illustration 3* convient dans la plupart des cas (type d'incident, pratiques de retour d'expérience, etc.). Certaines variations sont toutefois possibles. Dans la plupart des cas, ces variations ne modifieront pas la chaîne dans son

ensemble, mais elles méritent d'être prises en compte. Ne tenant pas compte des très rares exceptions dans la pratique (seuls un ou deux exploitants dans chaque pays), nous avons intégré ces variations dans la description des différentes étapes de la chaîne ci-dessous.

1ÈRE ÉTAPE : les premières données sont recueillies par le biais du centre de supervision du tunnel de l'exploitant. Les parties concernées soit effectuent des observations directes à l'aide des différents types d'équipements (télésurveillance, appels téléphoniques du public et communications radio, etc.), soit utilisent les enregistrements GTC (enregistrements des capteurs, enregistrements vidéo, etc.). L'opérateur basé au centre de supervision doit généralement s'occuper de cette tâche, qui peut toutefois être effectuée conjointement avec le gestionnaire dans certains cas. Lorsque des équipes extérieures (par ex. : police, pompiers) interviennent, elles recueillent souvent des données sur le terrain qui peuvent être identiques à celles recueillies par l'exploitant ou bien venir les compléter. L'organisation de l'échange des données entre l'exploitant et ces acteurs extérieurs varie. Dans certains cas, il existe un processus de partage des données (automatisé ou autre), et dans d'autres cas, l'exploitant du tunnel (généralement le gestionnaire du centre de supervision) organise des entretiens a posteriori. Les centres de supervision peuvent également être utilisés conjointement par l'exploitant du tunnel et une autre entité dont les équipes sont susceptibles de prendre des mesures en cas d'incident et/ou pour gérer la circulation (généralement la police). Dans ce cas, l'échange des données est simplifié.

2E ÉTAPE : les données initialement recueillies sont vérifiées puis modifiées et complétées si nécessaire. L'objectif est généralement d'éviter les erreurs (déformant la réalité), les données manquantes, les incohérences et le risque de divergences ou de doublons dans les données provenant de différentes sources. Les vérifications peuvent être effectuées par toute personne à différents niveaux hiérarchiques de l'exploitant, voire par plusieurs personnes à différents niveaux successivement. Les différents niveaux hiérarchiques correspondent au responsable du centre de supervision, au gestionnaire du centre de supervision (ou coordinateur du PC du tunnel), au responsable de l'exploitation et à l'agent de la sécurité. Certains exploitants de tunnels n'appliquent pas cette étape de vérification.

3E ÉTAPE : les informations requises par l'autorité nationale ou régionale sont extraites des données stabilisées par l'exploitant du tunnel. Il peut être nécessaire d'interpréter les données si les informations demandées par l'autorité ne sont pas directement disponibles à partir des données stabilisées après la phase de collecte. Normalement, l'exploitant du tunnel (généralement le responsable d'exploitation) préparera un rapport, en interprétant si nécessaire). Dans certains pays, l'exploitant soumet seulement les données et le rapport est produit par l'autorité administrative elle-même. Dans certains cas, quand le rapport est écrit par l'exploitant, celui-ci sera vérifié, voire rédigé (rare) par l'agent de sécurité. Ensuite, les données sont généralement expédiées par le gestionnaire de tunnel après vérifications (dans certains pays et pour certaines autorités, l'exploitant du tunnel envoyait les données). Dans certains cas, un circuit de transmission similaire peut exister entre l'exploitant du tunnel et le gestionnaire de tunnel et/ou le propriétaire du tunnel pour des rapports « *internes* » ou lorsque des informations spécifiques doivent être soumises à ce dernier.

2.4. DIFFICULTÉS POTENTIELLES À CHAQUE ÉTAPE DE LA CHAÎNE DE COLLECTE DE DONNÉES

L'objectif de ce chapitre est de fournir une courte explication des principales difficultés à chaque étape de la chaîne de collecte de données.

2.4.1. La collecte des données par l'opérateur de la salle de commande – 1re étape de la chaîne de retour d'expérience

Différents facteurs peuvent avoir une incidence sur la qualité de la collecte des données relatives à un incident.Tout d'abord, la charge de travail de l'opérateur lorsque la collecte des données aura un impact significatif. Cette charge de travail inclura la collecte de données en soi, et l'ampleur de cette tâche sera proportionnelle au nombre d'éléments de données requis. Même pour les données recueillies automatiquement, l'opérateur ou le responsable de l'exploitation doit vérifier les données et sélectionner celles qui sont pertinentes (vitesse d'écoulement de l'air, etc.). Pour certaines données qui ne peuvent pas être enregistrées à l'aide d'un outil automatique et/ou qui doivent être recueillies durant l'incident, les activités de collecte de données sont liées à d'autres tâches qui doivent être menées de front. Ces autres tâches sont généralement urgentes, importantes et prioritaires, car elles concernent directement la gestion de la sécurité des usagers impliqués dans l'incident. Elles sont par conséquent une source de stress pour l'opérateur.

Dans le cadre de cette gestion multitâche, la collecte des données n'est généralement pas une priorité et est également affectée par la façon dont l'opérateur perçoit l'utilité de ce processus. Cette perception dépendra de sa compréhension de la pertinence des données requises et de l'intérêt de l'incident derrière ces données. Le nombre de types d'incidents pour lesquels il convient de collecter des données peut en fait être élevé, allant des simples incidents techniques aux collisions et incendies qui font l'objet de ce rapport (cf. *chapitres 3 et 4*). Par ailleurs, certains exploitants de tunnels et autorités administratives exigent le même niveau de détail pour des incidents d'un niveau d'importance très variable (de la panne d'un système tunnel à la collision grave avec incendie à l'autre extrême).

La collecte des données doit généralement se poursuivre après l'incident, car les données initialement collectées doivent être complétées par les données collectées automatiquement par GTC et les données provenant d'autres sources (par ex. équipes de secours internes et externes).

Certaines informations importantes ne peuvent notamment être obtenues qu'a posteriori, par ex. décès des victimes dans une période de 30 jours[1] ou informations recueillies auprès de services extérieurs (pompiers, police, etc.). Si l'une des procédures de transmission des données (éventuellement automatisée) n'est pas disponible, il peut être nécessaire de contacter ces services, voire d'interroger les personnes impliquées dans l'incident. Cependant, ces acteurs disposent souvent de peu de temps, notamment les services de secours. Il peut donc être difficile d'obtenir les informations nécessaires et de s'assurer de la fiabilité de ces données (même les informations clés).

[1] La définition d'un décès consécutif à un accident de la route varie grandement d'un pays à l'autre et la période considérée, en particulier, entre l'accident et le décès n'est pas toujours la même. Selon la définition actuellement recommandée à des fins de normalisation, on entend par personne tuée dans un accident de la route : « *toute personne tuée instantanément ou qui meurt des conséquences de l'accident dans les 30 jours suivant l'accident* »

La collecte automatisée des données peut être utile pour délester l'opérateur d'une partie de son travail de collecte. Cela permet également à l'opérateur de vérifier ou de compléter ces données après l'accident sur la base de ses propres observations. L'automatisation n'est toutefois pas toujours la « *panacée universelle* ». En effet, une collecte automatisée des données sans vérification peut donner lieu à des erreurs directement liées à la capacité du système en termes de détection, de gestion des fausses alarmes, de mesures, de qualité d'acquisition et d'enregistrement (par ex. une trop grande distance entre les caméras). Elle peut également être totalement ou partiellement inopérante si le système technique en question ou un sous-système tombe en panne. Certaines données importantes peuvent difficilement être recueillies automatiquement (par exemple, celles liées au conducteur et/ou à la performance du véhicule). Ces données doivent donc être collectées de préférence par du personnel qualifié.

Si ces données initiales ne sont pas enregistrées ou si le résumé n'est pas clair ou difficile à comprendre, des erreurs peuvent survenir ultérieurement dans le processus. Des enregistrements manuscrits peuvent également poser un problème de ce point de vue.

Tous ces aspects peuvent affecter l'exhaustivité et la fiabilité des données initiales dans la chaîne de collecte de données.

2.4.2. Correction par le responsable de l'exploitation ou le gestionnaire de tunnel – 2e étape

Dans la pratique, cette étape est souvent négligée ou non systématique. Dans ce cas, des redondances peuvent subsister et avoir un effet négatif sur la clarté et l'utilisation des données. De plus, des contradictions entre les différentes sources de données ainsi que des données manquantes et des erreurs dans chaque source peuvent subsister. Cela peut affecter l'exactitude et la pertinence de l'analyse, au détriment de la qualité des statistiques découlant de ces données. Nous savons par expérience que même des données enregistrées automatiquement peuvent comporter des erreurs.

La période entre la collecte initiale et la correction des données est une priorité non négligeable. Comme le révèle le retour d'expérience, plus le temps s'écoule, plus il est difficile d'effectuer des vérifications/corrections. Il est notamment souvent nécessaire d'interroger les équipes internes (l'opérateur en particulier) ou des équipes externes à cette fin, et les souvenirs de l'événement peuvent s'effacer avec le temps. De plus, comme à l'étape précédente, les services de secours sont généralement occupés, ce qui complique davantage les vérifications.

Il existe différents types d'erreurs à vérifier : allant de l'erreur évidente (par exemple : un incident initialement enregistré en tant que simple panne qui en réalité a causé des victimes) aux cas plus compliqués dans lesquels il est difficile de déterminer si les données sont exactes ou erronées et où toute tentative de correction risque de déformer les faits.

Tout comme à l'étape précédente, l'ampleur des vérifications requises est proportionnelle au nombre de types d'incidents concernés, ce qui peut avoir un effet négatif.

2.4.3. Interprétation et transmission aux autorités par les exploitants de tunnels ou le gestionnaire de tunnel – 3e étape

Certaines informations requises par les autorités peuvent s'obtenir directement à partir des premières données collectées (par ex. nombre et types de véhicules). Toutefois, d'autres informations peuvent exiger la corrélation de plusieurs données, voire une interprétation et une analyse (par ex. facteur ayant contribué à la collision).

Dans certains cas, ces informations sont difficiles à établir et cette difficulté augmente proportionnellement au temps qui s'est écoulé depuis l'accident.

De plus, cette phase d'interprétation/analyse constitue une charge de travail supplémentaire pour l'exploitant du tunnel.

Enfin, l'exploitant du tunnel et son équipe peuvent ne pas être en mesure d'utiliser directement ces informations. Ils peuvent par conséquent ne pas en comprendre les avantages. Le personnel chargé d'élaborer et de transmettre ces informations peut par conséquent ne pas effectuer cette tâche conformément aux exigences, notamment s'il est en charge par ailleurs d'autres tâches.

Ainsi, ces informations peuvent n'être transmises qu'en partie, voire être omises.

2.5. AMÉLIORATION DES PROCESSUS DE COLLECTE DE DONNÉES ET LA CHAÎNE DE COLLECTE DE DONNÉES

2.5.1. Garantir la cohérence des données entre chaque étape de la chaîne de collecte de données

Pour les raisons expliquées au *chapitre 2.4.1*, si les types d'incidents (y compris les incidents non significatifs) à couvrir et les données à collecter sont nombreux, la charge de travail qui en découle pour l'équipe intervenant dans la chaîne de collecte des données peut être élevée, d'où un risque de démotivation. Une telle situation peut réduire la qualité du traitement des données (collecte, vérifications, interprétation, transmission) et, au bout du compte, également du produit final.

Ce problème peut être résolu en partie en embauchant davantage de personnel ou en prévoyant davantage d'équipements pour automatiser et améliorer la fiabilité de la collecte de données. Cependant, le renforcement de la capacité du personnel et des équipements pour améliorer la gestion des données relatives aux incidents peut ne pas être la solution prioritaire en raison de restrictions financières. De plus, cela peut ne pas être justifié du fait que les avantages sont limités, tant que la collecte et l'évaluation des données ainsi que leurs objectifs sous-jacents ne sont pas coordonnés de la meilleure façon possible.

Avant d'envisager d'augmenter les ressources allouées à la collecte des données, il semblerait donc opportun de réexaminer la pertinence des données et le niveau de détail requis ; et de s'assurer de la cohérence entre chaque étape de la chaîne de collecte de données. La cohérence est particulièrement importante entre :

- la pertinence des détails des données par rapport aux objectifs de retour d'expérience (y compris les objectifs de produits) pour l'exploitant du tunnel, le gestionnaire de tunnel et les autorités ;
- la pertinence de l'incident par rapport aux objectifs de retour d'expérience. Des critères d'évaluation doivent être établis (par ex. niveau de gravité, nouveaux facteurs, etc.). Par exemple, certains éléments de données peuvent être pertinents pour un accident corporel impliquant plusieurs véhicules, mais moins pertinents pour un impact avec des équipements impliquant un seul véhicule avec des dommages matériels uniquement ;
- la concentration sur les données qui peuvent être obtenues avec un effort raisonnable par l'exploitant du tunnel compte tenu de ses autres obligations durant une urgence et les capacités du système de sécurité. Il en va de même pour l'acquisition de données auprès d'autres sources internes ou externes (pompiers, police, etc.) ;
- la concentration sur les données qui peuvent être obtenues avec un effort raisonnable par l'exploitant du tunnel (correction par le responsable d'exploitation ou le gestionnaire de tunnel, interprétation et transmission par l'exploitant du tunnel aux autorités).

Pour améliorer la cohérence entre les étapes de la chaîne de collecte de données, il convient tout particulièrement de définir les objectifs de retour d'expérience (y compris les objectifs en matière de produits). Cela aidera à définir les données à recueillir, puis leur exhaustivité et leur niveau de détail.

Les différentes étapes de la chaîne de collecte de données sont interdépendantes. Il est donc préférable que les différents intervenants (personnel de l'exploitant du tunnel, gestionnaire de tunnel et autorités) coopèrent étroitement et définissent les objectifs de retour d'expérience et les critères d'évaluation (par exemple : pertinence de l'incident, élément de données et détails, etc.) ensemble. Il est nécessaire que chaque partie prenante identifie au préalable les avantages attendus de l'évaluation des données pour ensuite clairement définir ses objectifs de retour d'expérience. Si nécessaire, ces objectifs doivent être réexaminés au bout d'un certain temps pour optimiser le processus de gestion des données relatives aux incidents.

Le présent rapport (et souvent les objectifs de l'autorité également) ne se rapporte qu'aux incidents significatifs. Il est toutefois important de ne pas tenir compte que de ce type d'incident, notamment au niveau de l'exploitant (voir également les définitions dans le *chapitre 1.2*). Il est en fait préférable d'envisager la collecte des données dans son ensemble, ne serait-ce que pour évaluer la charge de travail y afférente. Ce processus d'examen doit donc intégrer de préférence tous les types d'incidents concernés par les données, qu'ils soient significatifs ou autres.

Ces examens peuvent amener l'exploitant du tunnel à augmenter les ressources humaines ou techniques affectées à la chaîne de collecte de données. Cette augmentation ne sera toutefois justifiable aux yeux des bailleurs de fonds et des équipes que si chaque élément de données est associé à des objectifs clairs et adéquats.

Dans la mesure du possible, cet examen doit associer des représentants des personnes chargées d'accomplir efficacement ces tâches (collecte, vérifications, etc.) dans une culture juste [45]. L'idée est de s'assurer de l'absence d'obstacle dans l'accomplissement de ces tâches.

Cet examen doit devenir avec le temps un processus actif. Par exemple, quelques années de pratique peuvent révéler qu'un ou plusieurs éléments de données ne sont finalement presque jamais utilisés ou peu pertinents pour les objectifs de retour d'expérience. Ces données peuvent alors être retirées du processus de collecte ou être remplacées par d'autres informations plus pertinentes.

Ces examens peuvent déboucher sur la nécessité d'un arbitrage délicat. Un principe peut aider : conformément aux objectifs de collecte de données, il semblerait préférable d'acquérir moins de données par incident et d'améliorer plutôt le nombre d'incidents sur lesquels des données sont collectées pour avoir une meilleure vision d'ensemble. Cela pourrait même conduire les parties prenantes à revoir une fois de plus les objectifs de la collecte de données et peut-être à en choisir de moins ambitieux et de plus atteignables et raisonnables en termes de ressources et d'avantages en termes de sécurité. Il est possible d'adopter une approche coût-bénéfice.

La collecte automatique des données peut contribuer à réduire la charge de travail de l'opérateur. Il convient toutefois de veiller à ce qu'une approche automatisée n'entraîne pas une sélection moins rigoureuse des données collectées. En fait, la collecte automatique des données représente aussi une charge de travail, notamment en termes de vérifications et de traitement. Comme cela l'a été souligné au *chapitre 2.3.1*, cette approche a ses limites en termes de fiabilité (par exemple, il est difficile de concilier une détection optimisée avec un niveau bas de fausses alarmes ; incertitude du capteur, etc.).

Comme indiqué au *paragraphe 2.3.4*, dans certains pays où les exploitants de tunnels sont peu nombreux et présentent une certaine homogénéité entre eux, une seule base de données est utilisée pour l'ensemble de la chaîne de collecte de données (de l'opérateur aux autorités). La 3e étape pour l'exportation, l'interprétation et la transmission des données par l'exploitant du tunnel à l'autorité peut être considérablement simplifiée : d'où l'avantage évident de cette pratique. Cependant, il est nécessaire avec cette pratique d'exporter directement toutes les informations requises par l'autorité à partir de cette base de données ou pour que l'autorité interprète les données (de préférence en coordination avec l'exploitant du tunnel). Par ailleurs, dans les pays où les exploitants de tunnels sont nombreux, avec une grande variété de pratiques et de ressources, il peut être compliqué d'adopter cette pratique. L'exigence minimale, dans la mesure du possible et en fonction des objectifs, est d'essayer d'harmoniser les données recueillies et les informations requises par l'autorité, c'est-à-dire limiter la charge de travail inhérente à la 3e étape de la chaîne de collecte de données.

2.5.2. L'importance de convaincre les parties prenantes de la pertinence de la collecte des données

Des restrictions réglementaires ne sont pas toujours appropriées pour garantir la qualité de la collecte et de la transmission de données. Certaines stratégies (qui ont été observées) consistent à cibler le minimum de données à fournir pour paraître conforme, par exemple, en ne déclarant qu'un certain pourcentage d'incidents significatifs.

Il est donc important que, pendant toute la durée de vie du tunnel, l'ensemble des parties prenantes et du personnel des exploitants de tunnels, notamment les personnes directement concernées, soient convaincus de l'importance et de la pertinence :

- de la chaîne de collecte de données et de ses objectifs,
- des données à recueillir et des informations à transmettre à l'autorité.

Tous les participants, de l'exploitant du tunnel au chef de l'organisation, doivent être impliqués.

Quelques méthodes pour convaincre les personnes concernées sont décrites ci-dessous.

Tout d'abord, il convient d'expliquer et de souligner les objectifs et les avantages de la chaîne de collecte de données ainsi que le rôle de chaque partie dans le processus de collecte de données et/ou la transmission des informations à l'autorité.

Deuxièmement, il semblerait nécessaire de justifier la pertinence de chaque type de données requises. Il ressort d'entretiens informels et des pratiques, par exemple, que les exploitants et gestionnaires de tunnel ont tendance à être moins disciplinés avec les données qu'ils considèrent comme inutiles. Ces données peuvent toutefois être importantes pour des raisons dépassant les activités de leur unité organisationnelle qui ne leur ont pas été expliquées. Il est donc recommandé de fonder ces justifications sur les processus de sélection de données expliqués au *paragraphe 2.5.1*. Il pourrait être très utile de mettre en avant ces explications en montrant ce que la collecte de données a permis d'obtenir en termes de résultats, comme l'amélioration des mesures, une meilleure appréciation des risques, la réduction de la gravité des incidents, la réduction du nombre de pannes techniques, la réduction du temps d'indisponibilité du tunnel, etc.

Troisièmement, sous certaines dispositions contractuelles, des exploitants sont soumis à des pénalités en cas d'accidents, des incidents et des fermetures de route. Ces pénalités peuvent induire en erreur un exploitant à ne pas enregistrer ou transmettre les détails d'un incident (bien sûr s'il y a un accident mortel, il ne peut pas être caché). Ainsi, il serait préférable d'éviter ce type de pénalités et préférer une approche de la «*juste culture*» qui au contraire aidera à établir une atmosphère de confiance en laquelle les parties prenantes sont encouragées (même récompensée) pour fournir des informations essentielles concernant la sécurité.

Enfin, il pourrait être utile d'insister sur le fait que les risques juridiques d'un retour d'expérience inapproprié peuvent être plus élevés qu'un retour d'expérience qui aurait mis en évidence des carences en termes de gestion de la sécurité. Il ressort de certaines procédures judiciaires pour des incendies majeurs survenus dans des tunnels que les verdicts sont plus sévères lorsque le processus d'amélioration et d'évaluation du système de gestion de la sécurité est inadéquat. Le retour d'expérience reste néanmoins la pierre angulaire de ce processus d'amélioration, et la gestion des données relatives aux incidents sa fondation.

2.5.3. Conseils pratiques

Certaines recommandations pratiques peuvent améliorer le processus de collecte de données. Certains exploitants de tunnels en ont déjà mis en œuvre.

Il semblerait approprié de consulter l'agent de sécurité[2] dans le processus de vérification des données (et clairement dans le retour d'expérience plus généralement), notamment avant la transmission des informations requises par l'autorité de contrôle. Compte tenu de l'indépendance nécessaire de l'agent de sécurité et de sa mission, il est préférable de ne pas l'associer directement aux tâches de traitement des données (exportations, interprétation, rédaction des rapports, etc.).

Des stratégies simples d'organisation de la collecte des données dans le temps peuvent être envisagées. Par exemple, lorsque l'opérateur de la salle de commande gérera l'événement, il se concentrera sur la collecte de certaines données en gardant à l'esprit que la priorité est la gestion de la sécurité. D'autres données seront obtenues ultérieurement à l'aide d'autres sources de données, par ex. des enregistrements du système automatique.

Cette stratégie d'organisation dans le temps doit toutefois être minutieusement préparée en termes de fiabilité et d'exhaustivité des priorités pour les différentes sources de données. Cette stratégie doit s'inscrire dans une approche globale associant toutes les parties prenantes à la collecte de données. L'objectif est de parvenir au parfait équilibre entre une collecte redondante (où les parties prenantes pourraient collecter les mêmes données) et une répartition de tâches de collecte spécifiques. La redondance accroîtra la charge de travail liée à la collecte de données, mais elle garantit des niveaux de fiabilité supérieurs grâce aux contrôles croisés. D'autre part, alors que la répartition des tâches permet de partager la charge de travail de collecte entre les parties prenantes, les risques liés à la fiabilité des données sont supérieurs. Il convient d'examiner ces aspects au cas par cas, en ce qui concerne les ressources, priorités et objectifs de collecte de données.

Ces réflexions peuvent être guidées par l'importance des données et la difficulté de les obtenir. Les données plus difficiles à obtenir peuvent être collectées durant l'accident et les données critiques doivent être systématiquement recueillies de manière redondante.

Certaines données dépendent plus ou moins des observations personnelles faites par les opérateurs de la salle de commande. Cela pourrait justifier le besoin de distinguer les données factuelles (par exemple : valeur d'un paramètre tel que la concentration en CO) des observations (par exemple : circonstances d'une collision). Aux fins de cette distinction, une observation pourrait désigner des données mises en contexte.

En ce qui concerne l'étape de correction (*chapitre 2.4.2*), pour gérer les erreurs non évidentes et le risque de « *corrections erronées* », il est recommandé de se doter d'une procédure claire (même courte) expliquant la façon de juger erronées les « *données suspectes* » et de décider de

[2] Le gestionnaire de tunnel désignera un agent de sécurité qui coordonnera toutes les initiatives de prévention et de sauvegarde pour assurer la sécurité des usagers et du personnel d'exploitation pour chaque tunnel d'une longueur supérieure à 500 m sur le réseau transeuropéen de transport. L'agent de sécurité agira de manière indépendante pour toutes les questions relatives à la sécurité des tunnels routiers et ne recevra aucune instruction d'un employeur en la matière.

leur élimination ou remplacement. L'utilisation des différentes sources disponibles est utile, mais pas suffisante. Pour les données plus critiques, des enquêtes supplémentaires peuvent être nécessaires. Par exemple, si le nombre de décédés varie d'une source à l'autre (du fait qu'un blessé qui décède dans les 30 jours soit compté comme tué dans l'accident), il peut être nécessaire de demander à la police[3] le chiffre à retenir.

Pour tous les exploitants de tunnels sur lesquels s'appuie ce chapitre, cette « *étape de correction* » est effectuée en interne par le responsable de l'exploitation ou en externe par le gestionnaire de tunnel. Il est également possible de faire appel à un tiers : une entité indépendante de l'exploitant du tunnel et du gestionnaire de tunnel qui pourrait intervenir dans cette « *étape de correction* ». Envisager cette possibilité peut être utile pour un exploitant de tunnel.

[3] Dans le cas des accidents mortels, c'est généralement la police qui détermine le nombre de morts.