ACCOUNTABILITY AND LIABILITY FOR 5G AND BEYOND – WAL5Gplus

Liability Management Based on Contracts

By Sylvie Jonas, Partner-lawyer at the Paris Bar
sylvie.jonas@agilit.law
06 67 07 36 57

Abstract: Contracts are a valuable tool, provided they comply with public policy provisions. Within a context of complex relationships or in the presence of numerous actors, contracts become even more valuable as a tool for managing roles and responsibilities. Once the contractual scheme of roles is laid out, a matrix of assigned responsibility can be drafted between the stakeholders. This matrix will describe the various commitments of each party in the construction and operational phases of the project. A Service Level Agreement can also be entered into by the parties, if they choose to, which will impact their liability.

I. Introduction

First, it's important to understand why 5G raises questions and issues in terms of liability:

Indeed, an important aspect to take into account when discussing liability management for 5G projects is how the characteristics of 5G affect liability management. 5G has specific characteristics that impact its use. Hence, it impacts liability expectations and commitments from users/clients.

Some of these characteristics are the fact that 5G is faster, offers a very low latency, allows for a greater number of connected devices per area, offers greater availability, etc. With 5G, we are going far beyond mobile internet. 5G allows far more applications that have different requirements in terms of service provisions and service level.

For instance, applications enabled by 5G include self-driving cars, assistance to medical operations, power plant management, critical communications, massive IoT deployment and interconnection, etc. For the most part, they will require strong guarantees from suppliers and operators.

This talk will not deal with the fact that 5G offers enhanced security. Indeed, the solutions that are enabled by 5G present an intrinsic risk, whatever the level of security has been designed to prevent. This risk must be dealt with through liability management.

Once we have discussed particular issues raised by liability in 5G projects, I will talk about how operators deal with liability regarding the network itself. I will also develop how contracts can be used to handle liability. And then I will talk about the tools already in place that can help deal with liability in 5G enabled solutions.

II. Liability regarding the network

A traditional mobile network is comprised of a radio access network, a core network and a transport network. The liability of the operator and the different parties involved will mostly depend on what the contract specifies. Certain regulatory exceptions may apply, such as the universal service or emergency call services.

This will result in a case by case analysis of each party's obligations. The operator might have the possibility of taking action against the responsible party based on the Contract if there is a contractual link or under fault-based liability.

For example, regarding Mobile infrastructure sharing[1]: the operator can take actions against the different operators under contractual liability if the different operators have signed an agreement regarding the sharing of such infrastructure. If the different operators have not entered into such contracts, the liability will be based on the fault of one or several parties.

The suppliers that provide services such as managing or implementing hardware or software will generally be subject to SLAs and availability requirements. If different operators or suppliers intervene on the core network for instance, a Responsibility Assignment Matrix can be most useful. This will be developed in part 3.

Clients that operate critical services need to prevent network failures from affecting customers and end users because of the dire consequences that such a failure can have: risk to image/reputation, loss of customers/market, but also damages to people and property.

[1] https://www.gsma.com/publicpolicy/wp-content/uploads/2012/09/Mobile-Infrastructure-sharing.pdf

With 5G, we see a reinforcement of the obligations that rest upon operators and suppliers. However, this is not surprising as 5G enabled applications will result in high stakes applications. The users/clients will wish to protect their applications by ensuring a high level of service from their operators and from their suppliers.

Clients that deal with an essential or critical infrastructures (such as banks) have regulatory obligations that they impose on their operators and suppliers. They will reinforce these commitments regarding applications and services based on 5G, such as they have already imposed on their outsourcing services through the Contracts.

Example of Outsourced Essential Services (in French *Prestataires de Services Externalisés Essentiels* (PSEE) which is a concept introduced by the CRBF (*Comité de la réglementation bancaire et financière*), the French Banking and Financial Regulations Committee, in its Regulation 97-02 of 21 February 1997: "Outsourced activities: activities for which the reporting company **entrusts to a third party**, on a permanent and regular basis, **the provision of services or other essential or important operational tasks**".

Outsourcing such activities comes with constraints and operational risks that need to be taken into account in the contract. **The purpose will be to ensure effective management capacity for the Client's activities. The contract will have to deal with the consequences of inadequate security of information systems.**

In this respect, the French Banking and Financial Regulations Committee specifies precisely that the functions delegated and performed by the service provider must remain under the control of the delegating company (ie. the client) and respect the principles defined by this Committee: Banks must therefore systematically set up Service Level Agreements. They shall include specific audit clauses such as the reproduction of the internal control system at the level of the service provider. This "permanent and periodic" control system (cf. *dispositif de contrôle « permanent et périodique »)* (as defined by the regulator) may be based on several quality standards: SAS 70 report[2], ISO standards, COSO or COBIT standards, etc. Additionally, the AMF (French Financial Markets

[2] SAS 70 (Statement on Auditing Standards no. 70) est une norme d'origine américaine reconnue au niveau international, notamment comme élément de conformité à Sarbanes-Oxley (loi US sur la responsabilisation des entreprises, lutte contre les comportements deviants et frauduleux des entreprises).
La norme SAS 70 a été créée pour définir les méthodes des organismes chargés du contrôle interne et des audits financiers sur les sociétés
Elle se caractérise par des audits indépendants réalisés par des tiers et des vérifications des processus sur site.
Cette norme concerne les entreprises qui font appel à des fournisseurs spécialisés pour externaliser leur service.

Authority) has introduced[3] the obligation to implement a business continuity plan (BCP) for providers of operational services that are "essential or important for the provision of a service or the conduct of business".

This example demonstrates how traditional contractual methods are efficient in dealing with situations where clients have reinforced requirements due to the critical nature of the service they provide.

This example illustrates how, similarly, 5G enabled solutions can be managed using:

1) Contracts. (See part 3).
2) Mechanisms such as Responsibilities Assignment Matrix, Service Level Agreements and penalties. (See part 4).

III. <u>Contracts</u>

The contract is a necessary tool: it sets out the roles and responsibilities of each party right from the recitals.

I will talk about a couple of contract clauses that should be edited to the manner used: recitals, purpose, phases of the project and liability.

3.1 Recitals

The recitals provide the opportunity to set out the background of the contract. The following is a list of a few points that may be developed in the recitals:

First point: the stakeholders

- Client
- 5G operator
- Equipment and service providers such as:
  - Equipment/hardware manufacturer
  - Reseller
  - Software manufacturer
  - Hosting service provider
  - Etc.

As an example, let us look at setting up a 5G virtual network for a hospital for its internal needs. We shall not examine the question of interconnection.

1st scenario:
A single contract entered into with just one partner (who may be the operator offering the virtual network). This contract partner will be in charge of coordinating all the parties involved and ensuring that these parties comply with their obligations under the Contract.

[3] Articles 313-56[3] and 313-72[3] to 313-75[3] of its Regulation (Book III. PROVIDERS, Chapter III. Organizational rules),

In the event of the virtual network malfunctioning, it will be easy to analyse the causes and attribute liability due to the fact that there is only one co contractor.

Similarly, with respect to IoT for example, the Client may:

- a/enter into contract with the operator, in which case it will be the operator who contributes the technology on which 5G is applied. Under these circumstances, the operator could be the client's sole partner.
  The operator will have to contract with the service provider(s) acting under the operator's responsibility.
  If the operator incurs liability due to the actions of the said service providers, the operator will have to seek reparation from these service providers based on the contracts.
  This set up is very cumbersome for the operator.
  To contain its liability and ensure that its client is involved in the project, the roles and responsibilities of the Client will also have to be defined: approval of the choices made by the operator, of the hardware and software etc.

- b/ enter into contract with a company which will provide all the connected technology including the dedicated network part. The company providing this offer will have very wide-ranging responsibilities and will need to:
  - a/ anticipate the possibility of having to seek reparation against third parties participating in the supply of the service (e.g. the operator) (in such a case there will be no impact on the Client but it represents an additional and complicated burden to be managed by the company providing the service); or
  - b/ manage cases in which its liability is sought in the event of loss related to the network: exclusions, limitations, mirror provisions to be reproduced in the contract to be entered into with the network operator.

2nd scenario:
A single contract that is multi-party. The contract is entered into between the client and all the entities taking part in the project. In such case, the contract will strive to distribute responsibilities between all the entities.

3rd scenario:

A set of separate contracts entered into between the Client and each of the participating entities:

- Hospital - telecoms operator agreement
- Hospital - integrator agreement
- Hospital - software suppliers agreement
- Hospital - hardware suppliers agreement
- Hospital - IOT supplier agreement

Scenarios 1 and 2 are the most comfortable for the Client. They avoid having each entity passing the buck in the event of malfunction.

The Responsibilities Assignment Matrix will be drawn up under the control and subject to the approval of the sole contract partner (scenario No. 1) or with concertation between the various relevant entities (scenario No. 2).

- The Recitals will also explain why the hospital wishes to have a 5G virtual private network: its expectations (against its current network), its requirements etc.

3.2 The purpose clause

The purpose clause will set out what the Client is buying and what the service providers are supplying. It seems easy in principle. And yet, I have often seen the purpose clause being the subject of negotiation. The requirements of the Client (what I am buying, or what I think I am buying) and the service(s) offered by the Service Provider(s) (what I am supplying for the price paid) are not always aligned with each other.

3.3 The phases of the Project

The Contract will govern two very distinct phases:

- a/ The build phase: the construction of the 5G virtual network
  For this phase, the following will, in particular, be the subject of negotiations:
  - the compliance standards used as reference;
  - compliance with the schedule;
  - mandatory milestones for which penalties may be incurred;
  - acceptance testing to ensure that the network established does comply with the Client's requirements.

- b/ The run phase: operating this 5G virtual network.
  With regard to the characteristics of 5G, the Client will have high expectations, especially in terms of availability. The availability of a network, whether 4G or 5G, is easy to measure and can easily form part of a Service Level Agreement (SLA). It is more difficult, however, to use an SLA for the security of a network. The Parties should therefore find an additional method of assessing the level of security.

The Liability-Aware Security Management for 5G could prove to be very useful here.

Pending these new forms of management of security and the corresponding liabilities, we are faced with several situations.

Let us imagine that the 5G virtual network breaks down:

- First scenario: the 5G network breaks down and the back-up solution(s) implemented by the operator work: an analysis of the causes will seek to find the element that has caused the breakdown and apply the agreed SLA, if necessary. We assert that in this scenario, the relationship between the various participants will remain peaceful since the impact on the final user is almost non-existent. In other words, the hospital is suffering a breakdown to its system but without any harm done to third parties.

- Second scenario: a breakdown of the hospital's 5G network and the back-up solution(s) fail. The hospital will suffer a very significant loss (impact on users, impact on patients, harm to image etc.).

    - a/ the cause can be identified and the supplier of the element that has caused the breakdown will have to indemnify the hospital under the terms set out in the contract. In particular, the limitation of liability provided in the contract will apply. In certain cases, however, this limitation may be superseded. In France, for example, a limitation of liability does not apply in the event of serious fault or misrepresentation;

    - b/ it is not possible to identify the cause, or the Parties do not agree on the cause. The contract may in such case provide for the appointment of an expert. Failing this, either Party may petition the court to appoint an expert. Another alternative is for one of the parties, if they consider that they have enough evidence, to refer the matter before a court with jurisdiction or, if the Contract has provided for arbitration, before an arbitration tribunal.

      Expert appraisal is a procedure that is lengthy and expensive. Likewise for court proceedings.
      There again it is necessary to investigate alternative methods of analysing the causes of a breakdown. Here again, the Liability-Aware Security Management for 5G might be of interest.

3.4 Liability

Liability will, of course, be a central issue.

In summary, with a single contract partner, the operator / service provider will:

- either take on the entire responsibility for the various intervening parties and personally deal with establishing their liability and seeking remedy from them; or
- limit or exclude its own liability in the event of fault or harm caused by the intervening third parties mentioned earlier.

The operator / service provider will have a real issue if they use open source software or off-the-shelf hardware because it will be difficult to include them in the contractual undertakings between the operator / service provider and the Client. It is important for the operator or service provider to obtain the client's approval for the use of open-source software or off-the-shelf hardware. The Client's attention should also be clearly drawn to the advantages and disadvantages of such use, in particular in terms of the warranties offered and liability. The best solution for an operator / service provider using such products should therefore be to ensure the limitation, or indeed, exclusion of its liability in the event of fault/harm/loss resulting from a breakdown of these products.

IV. Responsibility Assignment Matrix, Service Level Agreements (SLAs) and penalties

4.1 Responsibilities Assignment Matrix

A common issue in complex contracts it the allocation of liabilities between the different actors. This issue can be dealt with by using a responsibility assignment matrix.

Let's go back to our hospital example. Remember the hospital wishing to have a 5G private virtual network.

2 main scenarios will be considered:

- a/ the hospital will instruct various players on the basis of separate calls for tenders. One service provider to supply the dedicated 5G network (installation and management), another service provider to supply the connected hardware, another service provider to supply the software etc. There will be either one multi-party contract or several different contracts, **but in all cases it will be possible to use a responsibility matrix to manage this project overall both in the build and the run phases**;
- b/ The second scenario is the following. The hospital will instruct one service provider that will offer solutions to the entire spectrum of the hospital's needs. The solution will include the network, hardware, software etc.. Even in this scenario

and without any contractual undertaking by the various parties involved, a responsibility matrix can be useful. See its application below.

In order to use a responsibility assignment matrix, the first requirement is to determine what liabilities should be allocated to the different actors. This can be similar for all scenarios that we have mentioned before.

Then, the matrix requires the determination of how such liabilities are allocated. This will depend on the scenario.

A Responsibility Assignment Matrix describes the participation of the various stakeholders in a project. It's mostly a tool used for project management. It can be used to designate roles, responsibilities, and levels of authority for specific activities.

Traditionally, the Responsibilities Assignment Matrix will distinguish different roles (RACI), different tasks and allocate them between the stakeholders (ie. deciding for each task who is R, A, C or I):

- Responsible (R): Those who, in practice, do the work to achieve the task.
- Accountable (A): Those who are ultimately accountable for the correct completion of the task. The Accountable entity is the one that must approve the task delivered by the Responsible entity.
- Consulted (C): Those who are consulted before a task is achieved. The Consulted entity should voice their opinion (in a two-way communication)
- Informed (I): Those who are informed when a task is achieved (through a one-way communication).

In our hospital example, the following tasks/liabilities should be allocated (non-exhaustive list):

Build phase:

- Construction of the 5G network
- Supply of connected hardware
- Installation of connected hardware
- Connection of the hardware to the dedicated network

Run phase:

- Management of the 5G network
- Management of logging
- Maintenance of hardware
- Management of updates
- Response to warnings, incident resolution, escalation if necessary
- OS patching management

The way these responsibilities are allocated will vary in each of the different scenarios.

For example, in scenario No. 1, in which the hospital instructs various players on the basis of various separate calls for tenders, either through separate contracts or through one multi-party contract, the roles, Responsible and Accountable will be allocated to each player for the mission assigned to them. The Consulted entity may be allocated to the operator in certain situations where its approval may be required, for example for the approval of the connection to the network carried out by a third party. The C role may therefore be allocated to a party other than the one who has performed the tasks.

In scenario No. 2, where the hospital instructs a service provider who offers solutions to the entire spectrum of the hospital's needs., the distribution of the roles and responsibilities will be very different. While the Responsible entity will remain with the service provider who actually performs the task, the Accountable entity will for the most part be allocated to the service provider with whom the hospital has entered into contract.

Similarly, this service provider will more easily find himself in the Consulted role since they will play a coordinating role. The hospital for the most part will play the Informed role.

Should there be different actors, security obligations need to be formalized on interconnection issues. It can in fact be an entry point for a malicious third party for instance.

4.2 Service Level Agreements

Service Level Agreements can also be entered into by the parties. This is optional and will impact how they can be held liable. SLAs would not apply in a "build" phase, but would usually be used once the service is operational (that is to say, in the "run" phase). As such, this can affect two aspects of the suppliers/operator's liability:

- a/ Quality and availability of the services. This will be based on the definition established beforehand of quality and availability indicators, such as KPIs. In terms of a 5G network and applications based on a 5G network, the quality and availability of service would in practice be equivalent to an *obligation de résultat* [which means the obligation to provide results which is a form of strict liability under French law. Indeed, any deterioration in the service could result in serious consequences for the client and/or its final users, and may require indemnification of the loss.

- b/ The period within which the supplier/operator must acknowledge, process or resolve an incident. Allocation of priority levels to types of incidents is required. The Agreement shall set target time periods under which a response (acknowledge, processing or solutioning) of the supplier/operator is required.

In both cases, non-compliance with quality/availability requirements as well as with target time periods can lead to the application of penalties.

The field in which SLAs are now less effective is the area of security. There is therefore still lots of work to do to define SLAs that would be suitable for security.

Pending such progress, we consider that the obligation of security will remain what we call in French an *obligation de moyen* consisting, for example, of implementing all the resources that are relevant and necessary for the hardware, software and network components to reach a level of security that conforms to best practices. What will be sanctioned by the courts will not be the security failure itself. What will be sanctioned by the courts will be the security failure that occurred due to a failure to execute the resources and measures according to best practices and/or according to what was agreed upon in the Contract.

It is necessary to be vigilant with regards to the interconnection of an element that is poorly protected with a network or highly-secured hardware or software. The elements that are not secured or poorly secured may constitute an easy entry point into the network. It is fundamental to map all the elements of the network or those interconnected to the network.

4.3 Penalties

Delivery delays and/or lack of conformity with the responsibilities matrix and/or non-compliance with SLAs may give rise to penalties as stated in the contract.

The big question pertaining to penalties is whether they can be accumulated with damages.

It depends on the applicable law. It depends on what is stated in the contract.

Conclusion:

Today we covered:

- the liability regarding the network,
- the Contracts as a management's liability tool,
- the Responsibility Assignment Matrix, Service Level Agreements (SLAs) and penalties.

My recommendation would be to use the Contract as a valuable tool. For the Contract be a valuable tool, it should provide the parties with keys to determine who would be held responsible in the event of a Breach of Contract.

In the near future, the Liability-Aware Security Management for 5G will be a powerful tool. It's worth watching. Even possibly talking about in another workshop session!