2018). However, developing industry-specific rules that determine who has liability at each stage of a particular process may be needed in certain cases – e.g. in the case of letters of credit (see also Section 3.1(a)). In the case of permissionless blockchains, issues of jurisdiction and liability remain wide open.

Beyond the regulatory uncertainty surrounding the use of distributed ledgers, the deployment of Blockchain on a large scale could also be hindered by various standards and requirements imposed by national regulatory authorities, including data localization requirements and barriers to cross-border data flows.

(iii) Data localization and data privacy issues

The last few years have witnessed an intense debate over issues related to data localization, restrictions on cross-border data transfers and data privacy, with a growing number of countries adopting measures that impose requirements or restrictions on data flows.

According to the Information Technology and Innovation Foundation (ITIF), as of May 2017, 34 countries had enacted or proposed data localization requirements (Cory, 2017). Data localization requirements can take various forms. Data localization can be explicitly required by law or can be the result of a series of restrictions that make it *de facto* impossible to transfer data, such as local storage requirements, local processing of the data, or government approval to transfer data. Some countries prohibit all data transfers, while others target specific sectors or services. As for barriers to cross-border data flows, they typically involve restrictions on the transfer of personal data to jurisdictions deemed to provide a lower level of data protection, as well as limitations on information that governments consider "sensitive" (Cory, 2017).

Governments' motivations for putting in place such policies, which are increasingly raising concerns among the business community, which is wary of the implications for business activities, are diverse. Pursued objectives typically include addressing potential cybersecurity threats, promoting the local economy, ensuring access to data for the purposes of law enforcement, and protecting citizen's privacy.

To what extent are blockchain transactions likely to be affected by such policies?

As distributed ledgers, blockchain platforms are *de facto* relatively immune to data localization policies. Indeed, local storage requirements and local processing of data, which constitute the backbone of most data localization policies, are automatically met: one of the key principles of the blockchain technology is that all participants in the network have a local copy of the transactions and that every fully participating