Cloud computing is based on a paradigm shift with profound implications for computing ethics. The

main elements of this shift are: (i) the control is relinquished to third-party services; (ii) the data is

stored on multiple sites administered by several organizations; and (iii) multiple services interoperate

across the network.

Unauthorized access, data corruption, infrastructure failure, and service unavailability are some of

the risks related to relinquishing the control to third-party services; moreover, whenever a problem

occurs, it is difficult to identify the source and the entity causing it. Systems can span the boundaries

of multiple organizations and cross security borders, a process called deperimeterization. As a result of

deperimeterization, “not only the border of the organization’s IT infrastructure blurs, also the border of

the accountability becomes less clear” [350].

The complex structure of cloud services can make it difficult to determine who is responsible in

case something undesirable happens. In a complex chain of events or systems, many entities contribute

to an action, with undesirable consequences. Some of them have the opportunity to prevent these

consequences, and therefore no one can be held responsible – the so-called “problem of many hands.”

Ubiquitous and unlimited data sharing and storage among organizations test the self-determination

of information, the right or ability of individuals to exercise personal control over the collection, and

use and disclosure of their personal data by others; this tests the confidence and trust in today’s evolving

information society. Identity fraud and theft are made possible by the unauthorized access to personal

data in circulation and by new forms of dissemination through social networks, which could also pose

a danger to cloud computing.

Cloud service providers have already collected petabytes of sensitive personal information stored in

data centers around the world. The acceptance of cloud computing therefore will be determined by privacy

issues addressed by these companies and the countries where the data centers are located. Privacy

is affected by cultural differences; though some cultures favor privacy, other cultures emphasize community,

and this leads to an ambivalent attitude toward privacy on the Internet, which is a global system. The question of what can be done proactively about ethics of cloud computing does not have easy

answers; many undesirable phenomena in cloud computing will only appear in time. However, the need

for rules and regulations for the governance of cloud computing is obvious. The term governance means

the manner in which something is governed or regulated, the method of management, or the system of

regulations. Explicit attention to ethics must be paid by governmental organizations providing research

funding for cloud computing; private companies are less constrained by ethics oversight and governance

arrangements are more conducive to profit generation.

Accountability is a necessary ingredient of cloud computing; adequate information about how data

is handled within the cloud and about allocation of responsibility are key elements for enforcing ethics

rules in cloud computing. Recorded evidence allows us to assign responsibility; but there can be tension

between privacy and accountability, and it is important to establish what is being recorded and who

has access to the records.

Unwanted dependency on a cloud service provider, the so-called vendor lock-in, is a serious concern,

and the current standardization efforts at NIST attempt to address this problem.Another concern for users

is a future with only a handful of companies that dominate the market and dictate prices and policies.