Chapter 6

Gonçalo S. de Melo Bandeira
Escola Superior de Gestão, IPCA, Portugal

ABSTRACT

In Portugal, and in much of the legal systems of Europe, “legal persons” are likely to be criminally responsible for cybercrimes, for example, “false information,” “damage on other programs or computer data,” “computer-software sabotage,” “illegitimate access,” “unlawful interception,” and “illegitimate reproduction of protected program.” However, there are exceptions to the “question of criminal liability” of “legal persons.” Some “legal persons” cannot be blamed for cybercrime. The

DOI: 10.4018/978-1-4666-4526-4.ch006
1. INTRODUCTION

Criminal liability is the highest penalty that the modern democratic, free and true “rule of law,” gives to individuals and their organizations and/or “corporations, legal persons and similar entities.” Whether from the point of view of criminal law or from criminology perspective, or even in a trend of criminal policy, there is already a consensus, quite broad (Dias & Andrade, 1984; Dias, 2007). Quite broad consensus—in doctrine, jurisprudence, and legislation—on the necessity, appropriateness, and proportionality to consecrate the criminal liability of organizations—“corporations, legal persons and similar entities” (Bandeira, 2011a, 2011b; Guinter, 2009; Keulen & Gritter, 2010). Only a few voices in a few countries, like some doctrine in Germany, are still defending the old principle of “societas delinquere non potest” (Bandeira, 2004). But, even here, they have other type of sanctions. The criminal law—which is constitutional law—should always be a “law of minimum intervention.” A *ultima ratio* law. The criminal law, among other things, has to take into account the general and special positive preventions, but also the retribution and Justice. Some part of the criminal law must also look for a restorative Justice.

However, in the context of the Portuguese legal system, is scheduled to criminal liability of organizations (“corporations, legal persons and similar entities”) on different places of legislation, and in particular in the designated “law of cybercrime.” And this responsibility can in particular be for the following crimes: “False information”; the “Damage on other programs or computer data”; the “Computer-software sabotage”; the “Illegitimate access”; the “Unlawful interception” and “Illegitimate reproduction of the protected program”. It turns out that, with regard to the “criminal responsibility” of organizations, “corporations, legal persons and similar entities,” the “Law of Cybercrime” makes a reference to the Portuguese Penal Code.

We need to see also some of the possible legal consequences in relation to issues that are related to system administration information within organizations. And this, or that, is right in the middle of “corporations, legal persons and similar entities,” “organizations.” You need to check to what extent cannot exist here and there, an interception among the following three groups of questions. 1) “Management Information System” within organizations, *id est*, the “corporations, legal persons and similar entities”; 2) Responsibility/liability of the criminal organizations, *id est*, the “corporations, legal persons and similar entities” in the context of so-called “Cybercrime Law”; 3) Crimes of “False information”; “Damage on other programs or computer data”; “Computer-software sabotage”; “Illegitimate access”; “Unlawful interception”; and “Illegitimate reproduction of protected program.”

It is also crucial, of course, to realize how it works—from the strict point of view of legal technique and criminal—the nexus of imputation of criminal liability to “organizations,” i.e., the “corporations, legal persons and similar entities.” We refer to the respective criminal liability for