Chapter 30
Analysis of the Cybercrime with Spatial Econometrics in the European Union Countries

Vítor João Pereira Domingues Martinho
Polytechnic Institute of Viseu, Portugal

ABSTRACT

The main objective of this chapter is to analyze the crimes related to the new information technologies in the European Union using the data provided by the European Commission and the spatial econometrics approaches. The data were analyzed with several tests, namely the Moran´s I, to verify the existence of global (for all countries of the European Union) and local spatial autocorrelation. The presence of spatial autocorrelation in the data means that the variable analyzed in a determined country is auto correlated with the same variable in the neighboring countries. The data analysis was complemented with some cross-section estimations, considering namely the Lagrange Multiplier tests, to examine the spatial lag and the spatial error autocorrelation. The spatial autocorrelation is a statistical infraction, so the consideration of these subjects prevents result bias and on the other hand allows some conclusions important to help in the definition of adjusted policies.

INTRODUCTION

In our days the use of the electronic equipments and of the new technologies of information and communication increased enormously. These technologic improvements was good for our daily life, with new opportunities for economic advances and better development, as well social interactions, cultural exchanges, political evolution and others dynamics in another fields. In this context the internet appearance created a new world of challenges for everybody in every country. But, unfortunately, not everyone uses the new opportunities in the right way and today we have a lot of problems in the internet world, with some practices that cause many intentional damages for some people and/or organizations and in this framework we talk about the cybercrime.

The cybercrime appear associated namely with the emails fraudulent, racist message in the internet (blogs, online personal homepages, etc), online personal identity theft, critical information theft and/or destruction and financial transactions interference. This is a big problem because many

DOI: 10.4018/978-1-4666-6324-4.ch030

times and many people see their personal or organizational daily live affected with great prejudice and damage costs in their image and budget. In this way is urgent to develop a rigorous system of rules and laws, with adjusted number of institutions associated, to punish adequately the offenders.

Many countries, namely the United States of America and the European Union, developed a significant framework of rules and laws, as well new institutions to work in net, to prevent and avoid the cybercrime in the related countries. The preoccupation of the European Union, for example, is to create a network of cooperation among the different member states, try overcoming the problems that can emerge from the national boundaries and the related problems of the national jurisdiction. The European Union in the last decade defined a relevant number of rules with heavy prison sentences, namely for the offenders of the critical information system.

In this line this work presented here is an innovative research because analyze the cybercrime in an economic perspective and using spatial econometric techniques. There are not, of our knowledge, works that analyze the cybercrime with spatial econometric tools. These techniques, in the present study, allow us to determinate if there are spatial autocorrelation, or in other words, possibilities to investigate if the cybercrime in each European Union country is auto correlated with the cybercrime in the neighbors countries. If there are spatial autocorrelation, this statistical infraction must be taken into account in the data analysis and in the econometric estimations, if not the conclusions are bias. On other hand the analysis of the spatial autocorrelation give us important information helpful, namely to the definition of new policies.

Considering the context defined before, in this work we present, beyond this introduction, a literature revision, a data analyze, some spatial econometric results, some recommendations and finally the conclusions. The universe of analyze was the formerly 27 European Union countries through data of the year 2012, obtained in the Special Eurobarometer 390, because there are not many information about cybercrime, namely statistical information from official institutions.

BACKGROUND

The cybercrime analyze needs a multidisciplinary approach, considering that involve many problematic from many subjects. For example, considering the Routine Activity Theory (RAT), Kigerl (2012), in 132 countries, found that the richer countries with more internet users have a tendency to develop more cybercrime actions. On other hand, the countries with more unemployment usually have more internet users and more illicit internet activities. Holt and Bossler (2008) considered also the Routine Activity Theory to analyze the cybercrime occurrences, using a model where the dependent variable is the incidence of on-line cybercrime and the independent variables are the type of computer, the computer utilization, the type of protection and demographic factors (age, gender, employment, etc). Some of the findings support the predicted by the theory. The unemployment among the young people is seen by Kraemer-Mbula et al. (2013), in the actual crisis context as a favorable environment to increase the financial cybercrime, namely in the emergent economies like the BRICS. The national context of each country, namely at security, social, economic, cultural and politic, appear to be determinant for the application of international policies, specifically those related with the legal frameworks (Calderoni, 2010). For developing countries, Kshetri (2013) identified some determinants for the cybercrime, namely those related with the political and economic institutions (corruption, government poorly equipped and weak law adjustment), culture or informal institutions (nationalism and more condescending about the cyber-attack), human capital (less skills and education) and technology (less appropriated technology and less R&D).