ADCAIJ: Advances in Distributed Computing and Articial Intelligence Journal
Regular Issue, Vol. 6 N. 2 (2017), 85-95
eISSN: 2255-2863
DOI: http://dx.doi.org/10.14201/ADCAIJ2017628595

The online tourist fraud: the new measures of technological investigation in Spain[1]

M.ª Belén Aige Mut

Profesora Ayudante Doctora de Derecho Procesal. Universidad de las Islas Baleares.
Cra. de Valldemossa, km 7.5. Palma (Illes Balears) E-07122 Spain
belen.aige@uib.es

KEYWORD

Measures for the Technological Investigation; Online Tourist Contracts; Electronic Fraud

ABSTRACT

The present article is about an examination of the new technological measures for the investigation[2], created by the Organic Act (Ley Orgánica) 13/2015, of 5th of October. These measures will serve us to improve de criminal investigation, especially on those crimes that are done by technological means, but also for the traditional crimes. Specifically, we are going to make an especial reference to the tourist fraud, which affects both consumers and entrepreneurs.

This fraud is especially notable in the online contracts, as we will see above, because those contracts have increased the number of online frauds in the last years; in the tourism I am referring to the stealing of personal data and the creation of ghost companies or non-existent offers.

In first place, we are going to talk about the advantages and disadvantages of the online contracts, and also about the real necessity of new investigation means that finally have been satisfied with the introduction of the new technological measures of investigation, which we are going to analyse: the computerized undercover agent, the interception of the telematics and telephone communications, the recording of oral communications by electronic devices, the tracking, localization and recording images devices, the registry of mass storage devices and the remote registry of computer equipment.

1. The present work has been done within the framework of the Project «Big Data, Cloud Computing y otros nuevos retos jurídicos planteados por las tecnologías emergentes; en particular, su incidencia en el sector turístico» (DER2015-63595-R MINECO/FEDER), financed by the Dirección General de Investigación, del Ministerio de Economía y Competitividad de España.

The subject of this article was also treated in a Lecture called «Recientes reformas del proceso penal», which took place on December 14th 2015 in the headquarters of the Real Academia de Jurisprudencia y Legislación de las Illes Balears. Also, this subject was treated in a Lecture called «Las nuevas diligencias de investigación tecnológicas: especial referencia al sector turístico», which took place on October 19th 2016 in Salamanca, on the XX Congreso Iberoamericano de Derecho e Informática.

2. These new technological measures for the investigation are called «nuevas diligencias de investigación tecnológica» in Spain.

Finally, we conclude with a reflexion about the importance of these new measures today, without forgetting the disadvantages that also appear from them (especially, with the dispersion of data outside physical places and its introduction in the Cloud Computing). This is the reason why it is very important to obtain a correct interpretation and application by the Court.

1. Introduction

Nowadays, the tourist contracts are indispensable. Either for planning a vacation or for working, we will have to contract some kind of tourist service (accommodation or travelling). In my case in particular, the fact of living in an isle makes this necessity even bigger, which had been the principal motivation to make this study.

With the new technologies that are forming part of our lives, and becoming more and more natural to each one of us, it becomes a normal fact that we are going to do the contracts online. Those contracts, as we said in the abstract, have both advantages and disadvantages: on the good side they allow us to economize our costs and speed the procedures of the contracts, because we do not have to move from one place to another to do so; on the bad side there is still a big distrust on those means, because we have the feeling that something can easily go wrong. In addition, we keep observing more and more internet frauds that makes us even more suspicious.

For example, we know about the web pages that are false, the non-existent offers, the stealing of personal data (especially the bank data or the credit card data) …[3] All of those problems affect either consumer and entrepreneurs, as we said before, and misfortunately the claims are increasing every year, making it more necessary to obtain appropriate measures for the investigation, now more than ever.

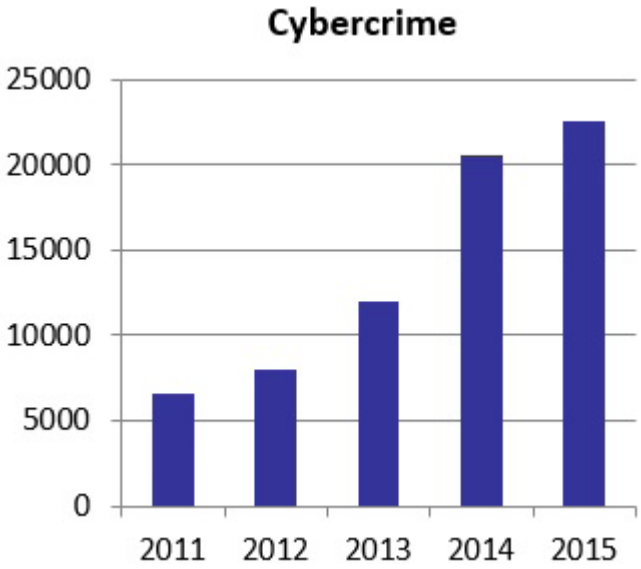
Until the recent reform of the Law, we did not have any suitable measure for the technological investigation, because our law was outdated since it was from 1882, and we had never have a good law reform of this subject. Fortunately, on October the 5th 2015, in Spain the Organic Act 13/2015 was approved, in order to modify the old Spanish Criminal Procedure Code (LECrim, Ley de Enjuiciamiento Criminal), strengthen the procedural guaranties and create the technological investigation means. This Law has introduced the new technological measures for the investigation, which are very important in cybercrime investigation.

I would like to begin by referring to the Annual Report of the Spanish Public Prosecutor (Memoria de la Fiscalía Española) from 2016[4] that reflects the increase of cybercrimes, in a total number of 22.575 for year 2015, an increase of 9.93% respect year 2014[5].

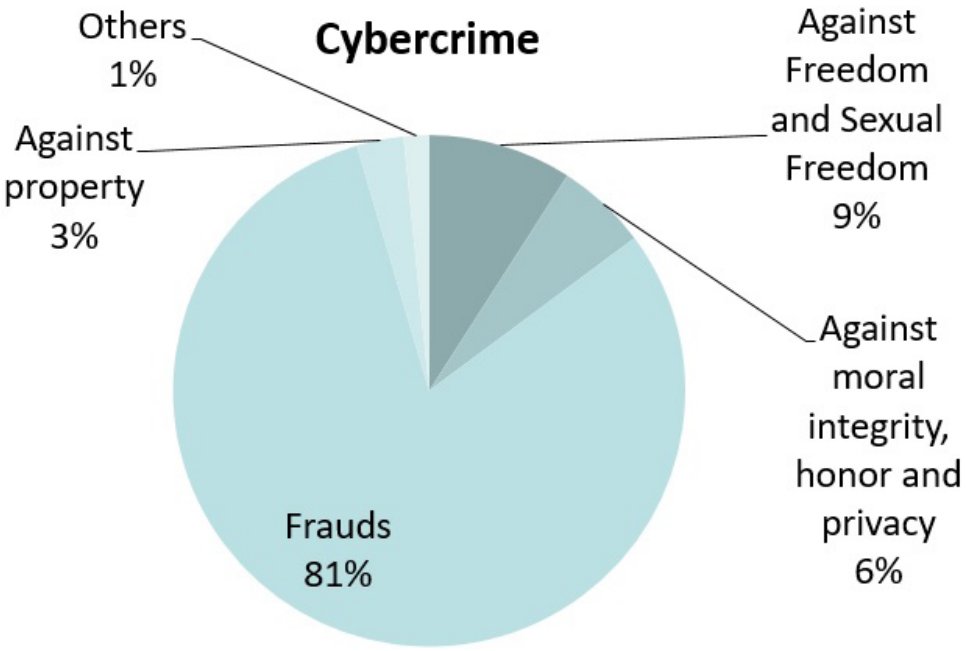
3. There are lots and lots of news about all of those types of fraud. For example: the closure of a low cost travel agency named «Tu tiempo libre» (DreamWings Tours), which had defrauded hundreds of people by charging the travel and not providing the services (obtained in the web page: http://cadenaser.com/ser/2015/08/19/sociedad/1439977676_821613.html [Date of reference: 9th of December 2016]); the fraud by a hacker of 1.8 million euros in air tickets by phishing, he obtained the north Americans GDS to generate travel tickets and then resell them cheaper (obtained in the web page: http://www.hosteltur.com/116574_hacker-estafa-18-m-billetes-avion-accediendo-gds.html [Date of reference: 9th of December 2016]); the appropriation by malware of personal data of the clients of an hotel, especially the credit card data (obtained in the web page: http://www.hosteltur.com/115313_ataques-internet-hoteles-van-apuntan-mejor.html [Date of reference: 9th of December 2016]); misleading massive offers by social networks like Facebook, as winning a travel by completing the personal data (obtained in the web page: http://www.hosteltur.com/112210_alerta-fraude-masivo-facebook-oferta-cruceros.html [Date of reference: 9th of December 2016]); etc.

4. This report can be consulted in the following web page: https://www.fiscal.es/memorias/memoria2016/FISCALIA_SITE/index.html [Date of reference: 9th of December 2016].

5. In 2014 the total number of cybercrimes were 20.534, which meant an increase of 71.21% respect 2013, and a total increase of 210% from 2011.



The most relevant crime among them is the cyber fraud, which includes the tourist fraud, with an 80.62% of the complaints (denuncias).



In the same way, the Spanish Ministry of Interior's Statistical Yearbook (Anuario Estadístico del Ministerio del Interior de España)[6] says that from a total number of 60.154 cybercrimes for 2015, 40.864 are cyber frauds

6. This report can be consulted in the following web page: http://www.interior.gob.es/web/archivos-y-documentacion/documentacion-y-publicaciones/anuarios-y-estadisticas [Date of reference: 9th of December 2016].

(a 67.9% from the total amount; with the credit card fraud being the most frequent, which affects to the online tourist contracts), of which only around 19.372 are solved[7].

Given the above, it is very important the creation of new forms of investigation and inquiry for these kind of crimes. These measures related to the new technologies are finally real and appear in the named LO 13/2015. These measures are the following:

1st) The computerized undercover agent (Art. 282 bis paragraphs 6 and 7 of the LECrim)
2nd) The interception of telematics and telephone communications (Art. 588 ter a) et seq. of the LECrim)
3rd) The recording of oral communications by electronic devices (Art. 588 quarter a) et seq. of the LECrim)
4th) The tracking, localization and recording images devices (Art. 588 quinquies a) et seq. of the LECrim)
5th) The registry of mass storage devices (Art. 588 sexies a) et seq. of the LECrim)
6th) The remote registry of computer equipment (Art. 588 septies a) et seq. of the LECrim)

There are a series of common provisions about these measures, except for the computerized undercover agent, which are collected in the Art. 588 bis a) et seq. of the LECrim. These common provisions, without any claim of completeness, are the following:

- The need of judicial authorization based on these principles: speciality (which means the investigation of specific crimes), suitability (by defining the objective and subjective scope, and its duration), exceptionality, necessity (we only apply these measures when there are no others less burdensome available and when they are really necessary for the investigation) and proportionality of the measures (when we adopt these measures we must weigh between the sacrifice of the rights and the benefit to the public and third parties interest).
- The secret concerning its adoption and all the subsequent actions of the requested measure.
- Concrete duration, specifically for each one of the measures.
- Control of the measure.
- Destruction of the original registries at the ending of the process by a final decision.

All of these measures are already in force in Spain since the 6th of December 2015, by the Fourth Final Disposition of the LO 13/2015. Now, we are going to analyse each one of them.

2. The computerized undercover agent

It appears regulated on the Art. 282 bis paragraphs 6 and 7 of the LECrim, as we said before. We need a judicial authorization to adopt it, and it has to be only judicial, not being possible an authorization of the Public Prosecutor (Ministerio Fiscal), which was possible for the traditional undercover agent. This authorization must be specific to the crimes collected in the Art. 282 bis paragraph 4[8] and for any of the crimes collected in the Art. 588 ter a)[9] of the LECrim.

7. It had been an increase from last year, which had a total amount of 49.966 cybercrimes, of which 32.842 were cyber fraud, 65.7% of the total amount. About that, the President of the Spanish National Court (Audiencia Nacional) told that usually only the 5.1% of the crimes are solved (one between twenty), in a Lecture in the «Congreso Internacional de Derecho Procesal Retos y Exigencias de la justicia (las reformas que nos vienen y las reformas necesarias)» which took place on 28th and 29th of October 2015 in Elche.

8. These crimes, about organized crime, are the following: felonies about trafficking and obtaining human organs, abduction, trafficking in human beings, prostitution, felonies against property and against social-economic order, felonies about intellectual and industrial property, felonies against the rights of workers and foreign citizens, trafficking in endangered species of flora and fauna, counterfeiting, arms trafficking, terrorism, felonies against historic heritage.

9. Intentional crimes punished by a maximum penalty of at least 3 years of prison, crimes committed under the wing of a group or criminal organization, terrorism and crimes committed by IT tools or any other technology.

So, this new regulation of the computerized undercover agent expands the scope of crimes more than the previously existing for the traditional undercover agent (those related to the organized crime). By doing that, it gives a bigger field of action and overcomes the idea of *numerus clausus* of the traditional undercover agent[10]. Anyway, this expansion of the crime catalogue seems too extensive, because a crime committed by IT tools or any other technology is enough to adopt this measure (as it fulfils its objective scope). If we go by the wording of the Law, we could even include any kind of crime regardless of its severity, for example we could include the tourist fraud that we are talking about, even if it is less severe. Because of that, in this area we have to specially evaluate the principles of speciality, suitability, exceptionality, necessity and proportionality, even if these principles are not directly applied to this measure by the common provisions that we talked about.

In the context of this measure, the judge can also authorize the obtainment of images and recording of conversations. With that, we connect this measure with the interception of telematics and telephone communications, among others, which suppose a very severe interference in the fundamental rights. Because of that and other reasons, we see that the computerized undercover agent suppose a bigger interference in the right to privacy and the privacy of communications (Valiño Ces, 2015)[11] and as a result of that we need exclusively the judicial authorization without possibility for the authorization of the Public Prosecutor.

3. The interception of telematics and telephone communications

This measure is included in the catalogue of measures that must apply the common provisions of the Art. 588 bis a) et seq. of the LECrim, so it must be adopted by a judicial authorization for the crimes collected on the Art. 579.1 of the LECrim[12] and the crimes committed by IT tools or any other technology.

We want to highlight in this catalogue of the Law the statement made in the Art. 588 ter a) *in fine* of the LECrim to «*crimes committed by IT tools or any other information and communications technology or communications service*». As Ortiz Pradillo says «*the Law uses an intentionally diffuse terminology*» (Ortiz Pradillo, 2015 [13] so it can let the door open to the changing state of the new technologies that will always progress faster than the legislative process.

Once again, as it happened with the computerized undercover agent, we must highlight the fact that inside the catalogue of crimes for this measure it is included the crime committed by new technologies. That makes possible to include the tourist fraud among the other crimes of the catalogue, but we must also observe that the fraud can be of little importance (in fact, as we said in the introduction, the most of the cybercrimes are frauds and these frauds can be large-scale or petty crime, even in the tourism, which can have a fraud by criminal organizations or small-scale frauds, as any other field). We think that is a little bit shocking to use this severe

10. It overcomes the problem of creating a restrictive list which was announced by Bueno de Mata, F., «El agente encubierto en internet: mentiras virtuales para alcanzar la justicia», Los retos del Poder Judicial ante la sociedad globalizada: Actas del IV Congreso de Derecho Procesal (I Internacional), A Coruña, 2 y 3 de junio de 2011 (Ana María Neira Pena, coord.), 2012, digital version obtained by the web page: http://ruc.udc.es/xmlui/handle/2183/9179.

11. Valiño Ces, A., «La actuación del agente encubierto en los delitos informáticos tras la ley orgánica 13-2015», en la comunicación realizada al Congreso Internacional de Derecho Procesal «Retos y exigencias de la justicia (las reformas que nos vienen y las reformas necesarias)», celebrado el 28 y 29 de octubre de 2015 en Elche, digital version obtained in the web page: http://congresoexigenciasjusticia.umh.es/comunicaciones-y-ponencias/.

12. The intentional crimes punished with a maximum penalty of at least 3 years of prison, crimes committed under the wig of a group or criminal organization and terrorism.

13. Ortiz Pradillo, J. C., «Desafíos legales de las diligencias tecnológicas de investigación», ponencia presentada en la mesa redonda *Medios de investigación tecnológica, del Congreso Internacional de Derecho Procesal «Retos y exigencias de la justicia (las reformas que nos vienen y las reformas necesarias)», celebrado en Elche los días 28 y 29 de octubre de 2015.* In that lecture he also said that because of the use of that diffuse terminology it is common to find terms in the Law such as «devices», «algorithms», «software», which are named by the state of technology so they can fulfil the constant changing development and save the legal obsolescence, as far as possible.

measure only because of that connecting link[14]. For that reason, we should apply strictly the principles included in the common provisions, once again: speciality, suitability, exceptionality, necessity and proportionality[15].

In emergency cases (which rarely appear in tourist sector, e.g. terrorism) it is possible the authorization of the Spanish Minister for Home Affairs (Ministro del Interior) or the Spanish Secretary of State (Secretario de Estado) that have to communicate it to the Examining Magistrate (Juez de Instrucción) in a maximum term of 24 hours in order to confirm or deny the measure in a maximum term of 72 hours.

An important innovation is that this measure can also authorize the access to the communication content and to the traffic data associated, which are the data generated as a result of the conveyance of the communication in a net of communications (for example the IMSI, IMEI, number, owner…). This possibility is very important because the data collection can often be more valuable than the communication content.

As a result of one of the previsions included inside de common provisions listed above, the measure will be controlled by the transcription of the most interesting excerpts by the Spanish Judicial Police (Policía Judicial[16]) as well as the delivery of the complete records (naming their origin and destination), but always by guarantying the authenticity and integrity with an advanced electronic signature (or other sufficiently reliable system of sealing and warning; therefore we can see with this last expression that the Law leaves again the door open to the advance of technologies not getting the fingers burnt with too exclusive definitions, as we said before)[17].

This legal reference to the advanced electronic signature (or a similar mechanism) is a right choice because other similar procedural laws in Spain, e.g. the Spanish Civil Procedural Law (LEC, Ley de Enjuiciamiento Civil) do not mention the systems that give authenticity and integrity to electronic documents, in cases such as evidence areas or Spanish monitorio procedural.

In order to end with this measure, we need to talk about another aspect of the common provisions: the duration. It is for a 3 months term, renewable to a maximum limit of 18 months.

4. The recording of oral communications by electronic devices

This measure is adopted by judicial authorization, as all the measures we are talking about that are under the common provisions of the Art. 588 bis a) of the LECrim. Also, it can be completed with the collection of images if it is specifically authorized in the resolution, this way linking with the measure of recording images, because the paragraph 3 of the Art. 588 quarter a) of the LECrim explicitly says that «*The interception and recording of private communications can be completed by the collection of the images when the judicial resolution specifically approves it*».

14. In the same way González Navarro, A. for the case of the remote registry of computer equipment, when she says that «*the fact that the crime is committed by IT tools (which can perfectly be a petty crime, as nothing is specified) is being equated with the use of this severe measure that we are studying*» (in spanish *«se equipara el hecho de que para la comisión del hecho delictivo se hayan utilizado las nuevas tecnologías con que para la investigación de los hechos (que perfectamente pueden ser de escasa relevancia, pues nada especifica el precepto en sentido contrario) se utilice una medida tan gravosa como la que aquí se estudia*»), González Navarro, A., «Nuevas tecnologías aplicadas a la investigación criminal: las regulaciones española y alemana», comunicación presentada en el *Congreso Internacional de Derecho Procesal «Retos y exigencias de la justicia (las reformas que nos vienen y las reformas necesarias)», celebrado el 28 y 29 de octubre de 2015 en Elche,* digital version in the web page: http://congresoexigenciasjusticia.umh.es/comunicaciones-y-ponencias/.

Moreover, this connecting link appears for many more measures for the technological investigation in the new Law, and we can do the same reflexion for them (as they can be very severe in certain cases).

15. We must specially apply the proportionality principle, which demands to limit the scope of the right's intrusion, depending on the case, as says Rodríguez Álvarez, A., «La intervención de las comunicaciones telefónicas y telemáticas: algunas dudas y reflexiones en torno a su vigente regulación», *Hacia una justicia 2.0. Actas del XX Congreso Iberoamericano de Derecho e Informática,* Ed. Ratio LEgis, Salamanca, 2016, p. 342.

16. Member of the national police assigned to an investigative judge and to the Public Prosecutor.

17. This control must also include the delivery of archives and not only recordings, because the intercepted communications can also be in written form, e.g. SMS, WhatsApp, as said by Rodríguez Álvarez, A., «La intervención de las comunicaciones telefónicas y telemáticas: algunas dudas y reflexiones en torno a su vigente regulación», *Op. Cit*., p. 350.

We think that this measure includes through the back door a truly measure of recording images in a private place, which is a measure that it is not included inside the specific measure of recording images (that it is only referring to open or public spaces, as we will see next).

To adopt the measure it is required the compliance of a series of requirements, on the one hand it must be connected to specific encounters and on the other hand it must fulfil all of the following requirements: it must be for investigation of intentional crimes with a maximum penalty of at least 3 years, crimes committed under the wig of groups or criminal organizations, or terrorism, and the collection of essential data with evidence base must be reasonably predicted.

In this case we can see that inside its objective scope, and because of the nature of the measure itself, it is more difficult to adjust the tourist fraud, although it cannot be discarded completely.

Continuing with the common provisions of the Art. 588 bis a) et seq. of the LECrim, the Judicial Police has to do a control of the measure by supplying the originals or electronic authentic copies to the judicial authority and by also giving the transcription. Regarding to the duration, the measure will be adopted for specific conversations, and will require a new judicial authorization for different encounters.

5. The tracking, localization and recording images devices

With this measure we are really talking about two different measures:

a) The recording of images in public spaces: this measure can be done directly by the Judicial Police by any technical means. As we said before, this measure does not refer to private places, so we have to adopt the measure of recording of oral communications by electronic devices previously analysed. Also, this concrete measure it is not very practical for the case of tourist fraud we are studying, because it will be rarely committed in open places.

b) The use of tracking and localization devices: this measure requires the judicial authorization in accordance with the principles of necessity and proportionality, and this authorization must always specify the technical media of realization. In emergency cases the measure can be adopted directly by the Judicial Police, with the commitment to inform the Examining Magistrate in a maximum period of 24 hours to confirm or deny it in the maximum period of 24 hours too. Its objective scope is not very specific because it only says «necessity reasons and proportionality of the measure», which is not very adequate because in this case we again leave the door open to any crime (even tourist fraud in which the measure can be necessary or proportionate, but it also cannot be; but we can clearly discard the emergency cases for tourist fraud).

The truly restrictive of fundamental rights measure in this case is the second one, the tracking and localization devices. Then, it is this measure that have to fulfil all the common provisions of the Art. 588 bis a) of the LECrim. In particular, about the duration it can be for a maximum limit period of 3 months, renewed by equal periods of time to a maximum limit period of 18 months. About the control, the Judicial Police will provide the original and copy when requested by the judge during the investigation and always at the end of it.

6. The registry of mass storage devices

This registry can be done during a domiciliary registry or even outside it, but it always require a specific judicial authorization and a different authorization to the access to the content. In emergency cases it can be adopted by the Judicial Police, which has to communicate it to the Examining Magistrate in a maximum term of 24 hours so it can be confirmed or denied in a 72 hours term.

The Art. 588 sexies a) paragraph one of the LECrim says that with this measure we can apprehend «*computers, telematics or telephone devices, digital mass storage devices or the access to telematics data repository*». That means we can access to the content of a BUS, portable hard drives, computers (laptop or desktop

computers) and mobile devices, all of them basic devices to the online tourist recruitment and also very important to investigate the tourist fraud (which is basically committed by online means).

We want to make a special reference to the mobile telephones, because nowadays they have a particular characteristic: they are smart, they are smartphones. In other words, in the same device we can do a lot of different functions (which can also be done by independent devices), for example, the smartphone can act as a camera, personal agenda, notepad, GPS, e-mail, telephone… So, many rights can converge in the same device: on the one hand the intimacy right (privacy) from the Art. 18.1 of the Spanish Constitution (CE), and on the other hand the privacy and secret of communications of the Art. 18.3 CE, which means that two types of different measures can also converge, the one about the registry of mass storage devices and the one about the interception of telematics and telephone communications (and even can converge the measure of tracking and localization devices).

The problem is that we must know if any of these measures is enough to access to all of the content of the Smartphone, or maybe if we need to adopt both measures. To obtain an answer, we must compare the requirements of one with another to see if they are the same or not.

For that matter, about the minimum content of the resolution, the control of the measure… they are all the same. Because of the nature of each one of them, of course the duration it is not applied to the registry of mass storage devices, but it is applied to the interception of telematics and telephone communications, which does not suppose a big deal. Where we see a major difference is in the area of the necessary judicial authorization, because in the case of the interception of telematics and telephone communications it can only be adopted for the crimes collected in the Art. 579 of the LECrim and also the crimes committed by IT tools, while the registry of mass storage devices can be adopted for any kind of crime (because there is no other rule), but in this case the judicial authorization must be specific for the registry of a mass storage device but also for the access to its content.

So, we can see that the two judicial authorizations do not match, and as a result only one judicial authorization cannot serve to adopt both measures.

The answer in this subject depends on the content we want to access from the Smartphone; thus, if we want to access to a content that only affects to privacy right (for example, the agenda, photographs, notes…) it is enough with the measure for the registry of mass storage devices, while if we want to access to a content that affects to the privacy and secret of communications (for example, the SMS, calls registry, WhatsApp, e-mails…) we must adopt the measure for the interception of telematics and telephone communications. With that precaution we can save the content obtained with the measure as a licit evidence in the process, not being an unlawful obtained evidence[18].

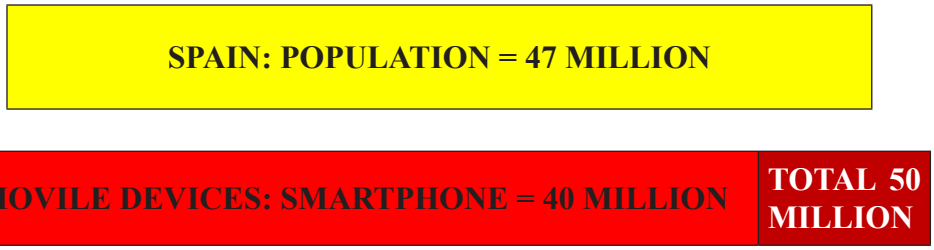
It is very important to find a right solution because in Spain, of a population about 47 million citizens according to the Spanish Ministry of Interior's Statistical Yearbook[19], we have more than 50 million mobiles[20]. Because of that, Spain is one of the most relevant countries in Smartphone penetration, with an 81%

18. Aige Mut, M. B. «El actual proceso de modernización de la Administración de Justicia: especial referencia a la nueva diligencia de registro de dispositivos de almacenamiento masivo», comunicación realizada para el *Congreso Internacional de Derecho Procesal «Retos y exigencias de la justicia (las reformas que nos vienen y las reformas necesarias)», celebrado el 28 y 29 de octubre de 2015 en Elche,* y digital version in the web page: http://congresoexigenciasjusticia.umh.es/comunicaciones-y-ponencias/.

19. Accessible, as said before, in the following web page: http://www.interior.gob.es/web/archivos-y-documentacion/documentacion-y-publicaciones/publicaciones-descargables/publicaciones-periodicas-anuarios-y-revistas-/anuario-estadistico-del-ministerio-del-interior [Date of reference: 20th of April 2016].

20. In April 2015, the number of mobile lines exceeded the 50 million, according to the Observatorio Nacional de las Telecomunicaciones y la Sociedad de la Información (ONTSI), which is the public corporate entity attached to the ministry of Industry, Energy and Tourism which is responsible for promoting the development of the Information Society in Spain) we can consult these actualized data in the Internet, by acceding to the following web page: https://data.observatorio.es/analytics/saw.dll?Dashboard&PortalPath=/shared/Indicadores%20Destacados/_portal/Indicadores_destacados&Page=Telefon%C3%ADa%20fija%20y%20m%C3%B3vil [Date of reference: 20th of April 2016].

of Smartphones over the total number of mobile devices, according to a report of the Fundación Telefónica[21]. Therefore, contrasting the previous data, today we have in Spain 40 million Smartphone[22].



What really matters is that most often the information contained on those devices is even bigger than the information that can be found in the domicile (Ortiz Pradillo, 2015)[23], which might cause an even bigger intrusion on the human privacy.

7. The remote registry of computer equipment

The Art. 588 speties a) of the LECrim says the following: «*The competent judge can authorize the utilization of identification data and codes, as well as the software installation, which allows, telematics and remotely, the distant examination, and without the owner or user knowing, of the computer's content, electronic device, computerized system, mass storage device of computerized data or database, as long as it fulfils the investigation of one of the following crimes:*» and those crimes are the crimes committed under the wig of criminal organizations, terrorism, felonies against minors or people with judicially modified capacity, felonies against the Constitution, treason and against national defence or crimes committed by IT tools.

If we can access without limits to the content of any kind of the previously mentioned devices, we could compromise a lot of rights, so we must act with precaution (as we said before with the Smartphone, in this case converge both rights and private secondary information). Because of that, all of the common provisions of the Art. 588 bis a) of the LECrim must be applied with caution, especially the principles of speciality, suitability, exceptionality, necessity and proportionality mentioned above.

Regarding the judicial authorization, and because of the intrusion of this measure, the Law requires a specific content authorization. That means it must specify the computers, electronic devices, computerized systems or their parts, computerized storage data means or databases or other digital contents which wanted to be accessed remotely; the range of the measure and its access and data or archives apprehension means, by naming the information control software; the authorized agents to execute it; the authorization to make and keep copies, where appropriate; and the precise integrity data preservation, inaccessibility or suppression measures. That means a very exhaustive control of the measure, as it has to be. And also knowing that, as the paragraph 3 said, the specificity of the authorization means that in case we want to registry another device or different part of a device, we must obtain a new judicial authorization.

21. Data obtained in the news «Spain, European leader in 'smartphones' penetration», published by the newspaper El Mundo on 22nd of January 2015, which can be consulted by the following link: http://www.elmundo.es/tecnologia/2015/01/22/54c0965c22601d656b8b456c.html [Date of reference: 20th of April 2016]. Those data reveal the clear and fast increase regarding 2014, year in which the smartphones were a total of 53'7%, according to the news titled «The Smart Phones win in Spain», published by the newspaper ABC on 29th of July 2014, which can be consulted in the following link: http://www.abc.es/tecnologia/20140729/rc-telefonos-inteligentes-ganan-espana-201407292059.html [Date of reference: 20th of April 2016]

22. The mentioned report from El Mundo also reveals that in Spain we have 23 million of active apps users, and that in the year 2014 more than 21'4 million Spaniards have acceded to mobile Internet. That means from the 40 million existing Smartphones, at least half of them, which is 20 million, are used with all of their potential of online connectivity.

23. Ortiz Pradillo, J. C., «Desafíos legales de las diligencias tecnológicas de investigación», *op. cit.*, there are some information that exist in the mobile phones but cannot be found in real life and, because of that we cannot access to this information with a traditional measure of entering and searching in a domicile, for example.

Concerning the duration, it is also very strict, because of the nature of the measure itself, and it is established in a maximum limit period of one month, renewable to similar periods to a maximum total of 3 months (it is the measure with the shorter term of the analysed measures).

With regard to the tourist fraud, it is hardly covered by the measure, but it can be investigated by it because of the expression «crimes committed by IT tools». Again, we question if this measure is proportionate, necessary and suitable for the tourist fraud, but it will depend on the case. We believe that this measure (which is very harmful for the fundamental rights) has an objective scope too open, and it gives the judge too much area of decision and arbitrariness to correctly apply all of the above mentioned principles (speciality, suitability, exceptionality, necessity and proportionality).

The creation of this measure is very important because the interception of internet communications can often appear with encrypted data, so we are going to need a decryption software which can affect human rights of the person investigated when introduced to a computer because that software could act as a spy software, some kind of a federal Trojan[24]. Because of that it is very important having an enabling rule that regulates this remote access possibility with a series of important limitations and restrictions.

8. Conclusions

It is obvious that we are in front of a completely necessary and important reform that is going to help a lot to the criminal investigation and that is going to simplify the correct realization of the investigation measures that affect the fundamental rights, so that later the Spanish Constitutional Court (Tribunal Constitucional) cannot revoke these measures because of legal faults. This new regulation is not only innovative but also very exhaustive and accurate, although it still is ambiguous in certain aspects, as could not be otherwise in the field of these actual topics. Other actual topics, such as Cloud Computing, are not regulated, and we will have to find an answer because most of these measures will be realized over devices that contain no physical information, since this information is hosted in servers by Cloud Computing, so we will have to combine several legislations from different countries in order to the good end of the investigation. And it is clear that we will have to wait until the application and interpretation of the Courts before we could make any more conclusions, but at least we have a previously non-existent but obviously unavoidable solid base.

Regarding the tourist fraud that it is analysed in this work, it is undeniable that these new measures will help a lot to its investigation and clarification, although not all the studied measures will be suitable because of its objective scopes (as we have been saying). We think that the more appropriate measures in this field will be the registry of mass storage devices (which could be completed, attending the severity of the crime, with the remote registry of computer equipment), the interception of telematics and telephone communications, and to a lesser extent the computerized undercover agent. With a correct application of those measures we could progress much more in the investigation of crimes committed by IT tools, which include tourist fraud.

9. Bibliographic index

Aige Mut, M. B., «El actual proceso de modernización de la Administración de Justicia: especial referencia a la nueva diligencia de registro de dispositivos de almacenamiento masivo», paper made to the *Congreso Internacional de Derecho Procesal «Retos y exigencias de la justicia (las reformas que nos vienen y las reformas necesarias)», celebrado el 28 y 29 de octubre de 2015 en Elche, 2015.*

Bueno de Mata, F., «El agente encubierto en internet: mentiras virtuales para alcanzar la justicia», *Los retos del Poder Judicial ante la sociedad globalizada: Actas del IV Congreso de Derecho Procesal (I Internacional), A Coruña, 2 y 3 de junio de 2011 (Ana María Neira Pena, coord.), 2012.*

24. González Navarro, A., «Nuevas tecnologías aplicadas a la investigación criminal: las regulaciones española y alemana», *op. cit.,* digital version on the web page:
http://congresoexigenciasjusticia.umh.es/comunicaciones-y-ponencias/.

González Navarro, A., «Nuevas tecnologías aplicadas a la investigación criminal: las regulaciones española y alemana», paper made to the *Congreso Internacional de Derecho Procesal «Retos y exigencias de la justicia (las reformas que nos vienen y las reformas necesarias)», celebrado el 28 y 29 de octubre de 2015 en Elche, 2015.*

Ortiz Pradillo, J. C., «Desafíos legales de las diligencias tecnológicas de investigación», ponencia presentada en la mesa redonda *Medios de investigación tecnológica, del Congreso Internacional de Derecho Procesal «Retos y exigencias de la justicia (las reformas que nos vienen y las reformas necesarias)», celebrado el 28 y 29 de octubre de 2015 en Elche, 2015.*

Rodríguez Álvarez, A., «La intervención de las comunicaciones telefónicas y telemáticas: algunas dudas y reflexiones en torno a su vigente regulación», *Hacia una justicia 2.0. Actas del XX Congreso Iberoamericano de Derecho e Informática*, ed. Ratio Legis, Salamanca, 2016.

Valiño Ces, A., «La actuación del agente encubierto en los delitos informáticos tras la ley orgánica 13-2015», paper made to the *Congreso Internacional de Derecho Procesal «Retos y exigencias de la justicia (las reformas que nos vienen y las reformas necesarias)», celebrado el 28 y 29 de octubre de 2015 en Elche, 2015.*

Consulted web pages

http://cadenaser.com [Date of reference: 30th of May 2015].
http://www.hosteltur.com [Date of reference: 30th of May 2015].
https://www.fiscal.es [Date of reference: 20th of December 2016].
http://www.interior.gob.es [Date of reference: 20th of December 2016].
https://data.observatorio.es [Date of reference: 20th of April 2016].
http://www.elmundo.es [Date of reference: 20th of April 2016].
http://www.abc.es [Date of reference: 20th of April 2016]