In Proceedings of the First Italian Conference on Cybersecurity (ITASEC17), Venice, Italy.

Rules of (digital) evidence and prosecution's actual needs. When the law falls behind technology

Andrea Monti
Adjunct Professor at the Master in System and Network Security
Rome University "La Sapienza"
lawfirm@andreamonti.net

Abstract

This paper analyses the evolution of the methods applied by the Italian Public Prosecution Service and Law Enforcement community to the digital investigations.

Starting from the early criminal trials, back in 1994, the paper shows how specific investigative trends have been anticipated by the "field necessity", and how the inability of the law to keep the pace with the rapidly-changing scenario led to mistrials and bad decisions that, to "save" a single trial, affected the legal system as a whole and the right to defense.

1 Introduction

> *Legal precedent in the field of digital investigations/digital evidence admissibility is burgeoning, resulting in digital forensic practices that are guided by industry standards developed from a mix of conjectural empiricism and anecdotal abstraction. In other words, our techniques are informed by what we think will be admissible and/or reliable based on how courts have ruled on other types of digital investigations or by analogizing to rulings on traditional evidence. In the absence of precedent, questions concerning "will the X evidence be admitted or carry weight if I do loom for digital investigators, and we are left with inefficient avoidance of risk. (Kennealy & Monti, 2005)*

More than ten years have gone by from when this statement was first written and high profile, computer crime related cases have been tried in court, but the current legal and technical problems of the digital investigations in Italy are still the same:

Forensics is still at an early-developed stage and the criminal Courts often tend to underestimate the relevance of properly acquired digital evidence, focusing more on the merit of the infringement. (RAND Europe, 2002).

Furthermore, network investigations are made difficult by old-fashioned criminal procedural provisions and a lack of training among the judges, prosecutors' services and the law enforcement community.

Facing the need to secure at (almost) any cost the result of a digital investigation and often lacking even a minimal understanding of the science behind the technology (Gennari, 2016), the courts - at all instances, up to the Corte di cassazione (Supreme Court) - have used their power of interpretation to allow technically questionable evidence to remain in the trial[i] or to fill either legislative or logistic gaps. (Monti, 2010)

Notwithstanding the 2008 update [ii] of the Italian Rules of Evidence by the enforcement of the 2001 Budapest Convention on Cybercrime[iii], a remote computer search or a data seizure still require heavy paperwork before even leaving the prosecutor's office, thus weakening the effectiveness of the investigation. And even when the "bureaucracy price" has been paid, the actual execution of the activities, as will be apparent in the next pages, much too often relies on the expertise of the private sector, as in the case of e-mail wiretapping, or website blocking.

Last but not least, the very promising 1.136.966 Euros EU funded *Cyber Tools Online Search for Evidence* (CTOSE) project launched in 2001 and ended in 2003 (European Commission, 2003), is now a webpage in Japanese dedicated to allergy issues (Allergy'sABC).

2 Digital Investigations' Technical evolution

2.1 The early days (1994 - 2000)

The core of the Italian digital investigative techniques was originally shaped by copyright and child pornography cases (Monti, 2004).

Early methods, dating back to 1994 during the Italian Crackdown (Gubitosa, 1999), involved the use of the Telemonitor TM 40 (a modem-to-modem wiretapping device), online covert activities to "engage" the system operators of the pre-Internet Bullettin Board System (BBS) and encryption to "seize" a part of a mass-memory without removing the whole computer (Chiccarelli & Monti, 2011).

None of the investigative techniques mentioned above included computer forensics methods of some kind because the then in force Criminal Procedural Code did not make it mandatory. Furthermore, the use of undercover law enforcement officers - allowed only when investigating drugs or weapon-related crime - was notwithstanding adopted in a copyright infringement case (the above mentioned "Italian Crackdown".) Not knowing exactly how to collect evidence of the software installed into a PC, the law enforcement officers made extensive use of the "print screen" command as the sole means to document what they did find during an *in situ* search. This poorly conceived method has been proven ineffective if not assisted by further verification.

The decision n. 1006/01 issued by the Court of Chieti on November 23, 2001 acquitted the defendant, charged with copyright infringement, because the Guardia di Finanza failed to check if the allegedly illegally installed software could actually run on the seized computer. During the trial, the Prosecutor-appointed digital forensic expert testified that the laptop technical specifications were much too weak to run the vector-graphics software installed. The implication of this technical assertion related to the manner in which the defendant could have used the software. The acquittal came out almost automatically.

While not allowed by the the law then in force, the use of undercover officers in a remotely-performed investigation was the hint of a real need and a *de facto* anticipation of the upcoming amendment to the limit of covert operations set forth in 1998 by the "child pornography act" (CPA).[iv]

CPA's Sect. 14 empowers the Polizia postale e delle comunicazioni (while not extending the possibility to the other law enforcement entities such as the Arma dei Carabinieri and Guardia di Finanza) to set up and manage undercover Internet child-pornography oriented websites or chat.

An interesting enforcement of the CPA comes from two child pornography cases investigated by the Prosecutors of Torre Annunziata (IT) and - separately - Catania, targeting a users' community hosted by Microsoft's MSN.IT.

A letter dated September 25, 2000, signed by Microsoft's Corporate Attorney EMEA reveals that the users' activity logfiles have been generated, collected and analysed in the USA, sent to Microsoft Italia and finally given to the Prosecutors. While, of course, there is nothing odd in the fact that a private company should cooperate with the Prosecution Service, the fact that the computer forensics has been performed in the USA on USA-based servers (while not even taken into account by the Prosecutor) anticipates the issues related to shortcutting the formality of the Criminal Procedural Code and the rules for the international judiciary assistance as emerged in the Pirate Bay case (see *infra*.)

2.2 Before the enforcement of the Budapest Cybercrime Convention (2001-2007)

A child pornography case that is strongly pertinent to this paper started in 2001 in Civitavecchia, Rome (IT), where the Polizia postale contacted a suspect on an IRC channel, exchanged some files - as allowed by the then recent legislation - and finally identified the young man suspected of being behind the remote monitor thanks to the information colletected during the IRC sessions. But what the Polizia postale forgot to do was to mark with a steganographic "sigil" that the images that were being sent to the suspect and to understand the legal implication of using IRC's Direct Client-to-Client (DCC) protocol.

The consequence of this carelessness would have been apparent a few years after. During the cross-examination, the police officer who handled the communication with the suspect acknowledged that the files sent to the suspect came from an internal police database used for this kind of investigation. Furthermore he acknowleged that no steganography had been used to make sure that what he sent was what the suspect actually received . The Court-appointed expert stated that according to his expertise, the exchange happened privately, via DCC and that Encase, the US forensics software used by the Polizia postale, produced a non-exact, bit-per-bit copy of the hard disk seized during the investigation, missing a whole part of the storage (while it has been impossibile to determine whether this failure was a defect of the software, an error of the operator or both.)

With such a flawed investigation, and in particular because the police did engage in an illegal activity [since covert operation aren't allowed by law in a private exchange (like IRC'DCC technically is)], on October 2004, 27 the Court of Civitavecchia decision n. 1277/04 declared null and void the evidence and acquitted the defendant.

This trial has been in many way crucial in the history of digital investigation.

First, it exposed the overconfidence of the investigators in their technical prowness. Secondly, it raised in court the issue of closed-source computer forensics tool, and third it pointed to the importance of remembering that during an investigation, the law comes first, even when surfing the Net. Had the police kept in mind that DCC is a point-to-point communication and that law doesn't allow covert activities in this case, the investigation would have possibly taken another path and maybe would never had landed in Court at all.

In the meantime, the public pressure on the child pornography issue led in 2006 to a regulation[v] that settled the "Centro Nazionale per il contrasto della pedopornografia sulla rete Internet - CNCPO" (National Centre for Online Child Pornography Contrast). Under this new law, the CNCPO is ordered

to maintain a website blacklist to be implemented in the Internet Service Providers (ISPs) DNSs to pre-emptively block the access to illegal contents.

In the same year, Parliament approved a similar provision targeting an online gambling website, and enforced the (now defunct) EU directive on online traffic data retention.

While not directly relevant to the digital investigations regulation, these laws grounded the idea, lately exploited by Public Prosecutors, that it was possible to block access to a website by hijacking the Internet traffic toward it.

Another element of interest of the child-pornography and online gambling traffic hijacking laws - together with the enforcement of the data-retention directive - is the cultural trend that keeps emerging: the privatisation of the criminal investigations and the necessary support role of the ISPs.

Obtaining logfiles from an ISP has always been the investigators' top priority. But the time constraints of the police activity (and the lack of training) led the authorities to adopt shortcuts that, in the long term, have backfired.

On March 2, 2006, issuing the final decision for a hacking case pending since 2001, the Court of Chieti (IT) stated that

> *... The investigation has been executed without deeper findings, because [the Polizia postale] just asked the ISP without any formal acquisition of the data and without any check about the data freezing to guarantee the evidentiary value in term of integrity and reliability over time. (Tribunale penale di Chieti, 2006)*

This decision is particulary relevant because it is the first to recognise, with no ambiguity, the need to adopt computer-forensics based investigative methods when accessing Internet traffic data.

The fact that the investigators tried to skip the formalities set forth by the Italian Data Protection Act - IDPA (Legislative Decree 196/03, sect. 132) is understandable while, of course, not excusable when facing multiple investigations that involve multiple ISPs and huge quantities of digital information. In these cases, strictly following the rules would prove to be a perfect way to stop chasing criminals.

To obtain Internet traffic data, the law enforcement officer must ask the Prosecutor for a written (i.e. paper) warrant which must be formally notified to the concerned ISP. If this notification is not made in person because the ISP is located somewhere else in Italy, the Prosecutor must send the written order to the local Police, Carabinieri or Guardia di Finanza headquarters to proceed with the formality. Otherwise the magistrate should authorize the use of any other remote communication means that guarantee the reliability of the notification. And when the order has been successfully notified, the law enforcement officers should perform, in person or with the help of a technician , all the activities necessary to extract the relevant information.

An empirical finding, based on the author's professional experience of the last twenty years, shows that there are several cases where law enforcement officers try to obtain access to Internet traffic data by simple fax or regular e-mail, refusing to go back to the prosecutor to ask for a formally correct order, and delegating to the ISP the technical activities of search and consignement of the data stored in the ISP's data-centre. Byzantinism of legal interpretation apart, this way of handling the Internet traffic data carries the risk of jeopardizing the upcoming trial, as the above mentioned case law shows.

Another interesting inside about the investigative techniques adopted by the Italian Public Prosecutors comes from the decision n. 1577/2010 issued on 2010, February 22 by the 7th Section of the Criminal Court of Milan.

The investigation for an alleged online defamatory publication started in 2003 and targeted the unidentifiable author of a series of articles related to the Italian VIP world. After about a year without having succeeded in discovering the true identity of the suspect, the Public Prosecutor decided to send a "poisoned" e-mail to the address used by the suspect that, once read, would have grabbed the client-related information, thus revealing the IP, the operating system, the browser and so on. Furthermore, the prosecutor relied upon social engineering to lure the suspect into opening the message.

Initially, this technique failed to provide any useful results because the suspect was hidden behind the NAT of his ISP, so the prosecutor ordered the setting up of a server with a static IP number inside the ISP's network and to have the "poisoned" e-mail linked to this IP. This way, once opened, the e-mail reveled the internal IP actually assigned to the user.

While a clever technique, it is hard to accept the idea, expressed by the decision, that this is a method that can be used without a Court warrant, solely upon the Prosecution's order because of the nature of "digital tailing". The technique adopted by the Prosecutor, indeed, is more akin to a some sort of wiretapping and thus – given the silence of the law - should have been treated as such.

The very same problem affected other decisions that, around 2008, had to deal with the legal notion of (some sort of) traffic hijacking as an investigative tool.

The Italian investigation started in 2008 against a website called *The Pirate Bay*, a Swedish based torrent engine whose owners were accused of copyright infringement, came to a sudden halt when the prosecutor of Bergamo (IT) realized that he had no jurisdiction in Sweden. In other words, there was no quick way to both collect evidence by way of a seizure and stop the ongoing "crime".

With what could be rightly called a semantic somersault, the prosecutor asked the Court conducting the investigation (Giudice per le indagini preliminari - GIP) for a seizure warrant of the Internet traffic against the Swedish server. Accordingly, the Court ordered

> *the preemptive seizure of the ... website, ordering that the ISP, and specifically those operating on the Italian soil ... prevent their users from accessing the address www.thepiratebay.org, its current and future alias and domain names, and any further static IP associated to the very same names, now and in the future. (Giudice per le indagini preliminari di Bergamo, 2008)*

The technical oddity of this decision is apparent: to seize something to somebody means taking the thing away from him, or preventing him from either accessing or using the thing. Asking third parties (the ISPs) to block other people (their customers) not involved in the criminal proceedings is frankly too much even for the most prosecutor-inclined among the judges.

A partially reversed judgement came a few weeks later on September 24, 2008, when the Tribunale della libertà (the appellate court for the GIP's decision) while confirming the Italian jurisdiction over the case, ruled against the possibility of extending the legal notion of "seizure" to include Internet traffic hijacking.

Finally, on Sept. 29 2009, the III Criminal Section of the Corte di cassazione, with the decision n. 49437, re-affirmed the Italian prosecutor's jurisdiction even if there were no evidence of an actual involvement of Italian citizens, by not excluding, in theory, this possibility and, with a convoluted and thus weak logic, sustained the very first interpretation of the law adopted by the GIP.

As always happens in the legal world, once a break is open into the granite wall of technology, everybody tries to sneak into the hole, no matter whether this make sense or not. So at the very same moment of the The Pirate Bay quarrel, other prosecutors and GIPs adopted the Bergamo Ruling.

On September 29, 2008 the GIP of Milan, upon the request of the prosecutor investigating a case of cigarette smuggling, issued a Bergamo-like Internet traffic hijacking order. A certain number of ISPs that were notified of the order tried to counter it by claiming its technical infeasibility but to no avail. On December 12, 2008 the Tribunale della libertà rejected the ISPs claim on the basis of a convoluted and technical unsavvy logic that affirmed the equivalence between seizing an object and preventig third parties to touch it. The very same logic enforced later by the Corte di cassazione in the final verdict on the investigation methods adopted by the prosecutor in the The Pirate Bay case. Following this lead, in the next year, seizure-by-traffic-hijacking became a standard, unchallenged operating procedure for every investigation involving network resources located abroad.

The common denominator of these decisions is that every player in the game acknowledged that the usual, paper-based investigation rules were simply unfit for the speed and the complexity of a criminal offence involving digital assets so, using the prerogatives that the law grants to the judiciary the judges *fecerunt de albo, nigro*. But by fixing a temporary problem, they opened the way to the

disruption of the legal notion of jurisdiction as geographical limit of the State's power, creating a reciprocity that could permit the authorities of other countries legitimately to shut down "disturbing" websites hosted in Italy.

2.3 After the enforcement of the Budapest Cybercrime Convention (2008-Today)

Notwithstanding the hype generated in the computer forensics community, the enforcement of the Budapest Cybercrime Convention didn't actually benefit digital investigations. True, digital forensics techniques have been elevated to "evidence status", but the non-use of these techniques has no consequences in Court because there is no provision that excludes the weakened digital evidence from the Court (Senor, 2012)

While a lot of attention has been paid to the digital forensics-related legal innovations, one of the Convention's core provision is the mandatory adoption, in every State, of a 24/7 network to realise effective, mutal cooperation for the investigation of transnational computer crimes. (Luparìa & Ziccardi, 2007, Luparìa, 2009). Needless to say, there is no trace of this 24/7 network that would have solved many (if not all) the jurisdictional problems that were raised early in 2000 by the Torre Annunziata and Catania's child pornography investigations and later by the Pirate Bay case (see *supra.*)

So far, therefore there is no evidence of a broad use of the digital investigation tools set forth by the Italian enforcement of the Convention. Many Public Prosecutors continue asking the ISP to provide, often by email, the suspect's traffic data and don't care about the need to adopt adequate measures to secure the information. It is, then, safely (and sadly) possible to say that the Cybercrime Convention just passed almost unnoticed in the Italian digital investigative system.

Nevertheless, a couple of cases involving the use of viruses by the Prosecution Service to collect digital evidences confirm the assumption that the dialogue between Law and Technology is (conveniently) a dialogue of the deaf.

In Italy, the use of viruses and malware to remotely retrieve content and information from a computer was first accounted (from the "wrong" side of the barricade) in the Telecom-Sismi trial (Pompili, 2008), but gained "public status" in 2015 with the Hacking Team scandal.

On July, 2015 the Milan-based IT security firm's internal emails were leaked into the "wild" by way of an illegal access to its systems. As a results, the public and the media discovered, "all of a sudden", that the Italian government's secret services employed malware designed by Hacking Team to perform its activities and stealthily gather information from remote computers.

While Galileo (this is the Hacking Team's software name) and its siblings are perfectly fit for the scope of gathering information for intelligence purposes, the "as is" transposition of its *modus operandi* in the criminal investigation domain is not so easy.

The main difference between the two realms is the role of the digital forensics.

While in the intelligence and military circles the use of digital forensics-grade techniques is a low priority because none of these information are supposed to ever land in Court, the very same approach doesn't work for the "regular" investigation where rules of evidence reign. (Mancini, Panico, & Monti, 2017).

Confronted with the Prosecution Service's use of a malware to hack into a mobile device used by a suspect to record his conversations, the Corte di cassazione exposed three times the specific techniques involved in these cases.

From the first ruling (Vth Branch, decision n. 16556, issued on 2009, October 14), it appears that in 2004 the Prosecutor of Palermo accessed the suspect's PC with the excuse of obtaining a copy of the file stored in the disk, while actually installing a backup utility verbatim named "gosth" - but more probably, (Norton) "Ghost", to be able to seize, from time to time, all the files newly created.

While the previous case didn't actually involve any malware, the ruling n. 27100 issued by the Corte di cassazione,VI branch on May, 26 2015 dealt with proper malicious software secretely installed in a smartphone, and used to wiretap the private conversations of the suspect.

About a year later, the Sezioni Unite (the assembly of all the single Corte di cassazione branch) issued the ruling n. 26889/2016, meant to be the definitive rule of law about the use of malware to eavesdrop private conversations. In this ruling, the Sezioni Unite didn't enter into the technical merit of the malware exploitation, limiting its analysis to the evidentiary value of the intercepted communication, and taking for granted that there were no technical issues to account for.

The last publicly known use of malware in criminal investigation (at the time of the submission of this paper) is reported by IlSole24Ore in 2016, October 10. (Monti, 2016.)

The Prosecutor of Modena installed malware into a server of a public authority , so to obtain a copy of all the emails belonging to the suspect. The technical aspects of the investigation have not yet been made public, so it is not known whether the malware simply copied the messages already downloaded locally, or if it actively accessed the suspect's Gmail account to retrieve the content from the USA (or wherever the files were located.) In this latter case, as in the Torre Annunziata and Catania 200's investigation, once again we would face an investigative activity performed outside the Italian jurisdiction, and unbeknownst to the authorities of the "targeted" country.

3 Lesson learned and Conclusions

The analysis of the parallel evolution of the digital forensics techniques and of the rule of evidence clearly shows that the legal framework is largely unfit to both ensure an effective investigation and respect of the rights of the defense.

When investigating minor crimes involving digital assets located abroad, the effort required to activate (when possible) the international cooperation with the authorities of other countries is paramount in respect of the damage suffered by the victim (this is especially true, for instance, in *phishing* cases.) The situation is aggravated by the growing number of (often trivial or petty) claims made by the public that overloads the response capacity of the Prosecution Service.

The pragmatic reaction of the justice and law enforcement communities is to widely use the power of interpretation to fill the logistic and legal gap of the Italian investigative rules, while there is no hint of a long-term strategy to mitigate the effects of the two above mentioned concurring factors that hinder the effectiveness of a computer-based investigation.

The effect of the disease is clear, the way to cure it, not. And the cure is still largely unknown because of the lack of reliable metrics on the contribution of digital evidence when the court issues its final verdict.

Without such kind of analysis there is no way to tell which forensics methodologies are sound enough to stand in court, or what is the bare minimum to grant the digital forensics outcomes a "trial evidence status", making impossible to draft a coherent set of legislative provisions. So we will continue the endless and useless quadrilateral confrontation among lawyers, magistrates, law enforcement and technical experts where every involved subject grounds his position either on personal beliefs or (limited) experience instead of relying upon figures and fact-checking.

The danger of this approach is that it trades short terms results (not always achieved) for bad caselaw whose verdicts are largely based on the (lack of) knowledge of a single magistrate rather than upon a strong and shared set of scientific principles applied to the decisional process.

By failing to recognize both the important scientific and technical aspects of the problem and the need of fair enforcement of the letter of the law, the road to justice is paved with mistrials and both innocents and culprits will be denied of the justice they deserve.

Works Cited

Allergy'sABC. (n.d.). *Difference and side effects of the effects of the anti-allergy drug*. Retrieved 10 1, 2016, from アレルギーに関するイロハ (Iroha on Allergy): www.ctose.org

Chiccarelli, S., & Monti, A. (2011). *Spaghetti Hacker* (2nd edition ed.). Pescara: Monti&Ambrosini editori.

European Commission. (2003, 09 30). *CTOSE*. (European Commission) Retrieved 10 1, 2016, from Community Research and Development Information Service: http://cordis.europa.eu/project/rcn/60288_en.html

Gennari, G. (2016). *Nuove e vecchie scienze forensi alla prova delle corti.* Milano: Maggioli editore.

GIP Bergamo - Decreto di sequestro preventivo, p.p. n. 3277/08 (Tribunale penale August 01, 2008).

Gubitosa, C. (1999). *Italian Crackdown.* Milan: Apogeo.

Kennealy, E. E., & Monti, A. (2005). Case study: A failure success' clothing. *Digital Investigation , 2* (4), 247-253.

Luparìa, L. (2009). *Sistema penale e criminalità informatica.* Milano: Giuffrè.

Luparìa, L., & Ziccardi, G. (2007). *Investigazione penale e tecnologia informatica.* Milano: Giuffrè.

Mancini, L., Panico, A., & Monti, A. (2017). *SOF on Trial. The technical and legal value of battlefield digital forensics in Court* . TBP.

Monti, A. (2016, October 10). Il virus trojan non sostituisce il sequestro. *IlSole24Ore* .

Monti, A. (2010, February 10). Notifiche irrituali nel sequestro ai pirati. *IlSole24Ore* .

Monti, A. (2004). The Legal Duty of IAPs to Preserve Traffic Data: A Dream or a Nightmare? . *INTERNATIONAL REVIEW OF LAW COMPUTERS & TECHNOLOGY , 18* (2), 221-230.

Pompili, A. (2008). *Le tigri di Telecom. La sicurezza italiana e le sue deviazioni attraverso un eclatante scandalo mediatico.* Roma: Stampa Alternativa.

RAND Europe. (2002). *Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries* . European Commission, Directorate-General Information Society , Brussels.

Senor, M. (2012). Informatica forense. In U. Pagallo, & M. Durante, *Manuale di informatica giuridica e diritto delle nuove tecnologie* (p. 251). Torino: UTET Giuridica.

Tribunale penale di Chieti - Decision 175/06, 2774/01 (Tribunale March 2, 2006).

[i] Court of Appeals of Bologna, decision n. 369 issued on 2008, January 08 - made public on March, 2008, 27 - http://www.ictlex.net/?p=692 - retrieved 2016, October 01.

[ii] *Legge 18 marzo 2008, n. 48 - "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno* published in *Gazzetta Ufficiale n. 80, 4 aprile 2008 - Supplemento ordinario n. 79* - http://www.parlamento.it/parlam/leggi/080481.htm - retrieved 2016, October 01.

[iii] The Convention on Cybercrime of the Council of Europe (CETS No.185), known as the Budapest Convention, is the only binding international instrument on this issue. It serves as a guideline for any country developing comprehensive national legislation against Cybercrime and as a framework for international cooperation

between State Parties to this treaty - http://www.coe.int/en/web/cybercrime/the-budapest-convention - retrieved 2016, October 01.

[iv] *Legge 3 agosto 1998, n. 269 Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitu'* published on *Gazzetta Ufficiale n. 185 del 10 agosto 1998* - http://www.camera.it/parlam/leggi/98269l.htm - retrieved 2016, October 01.

[v] Legge 6 febbraio 2006, n. 38 *Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet* published in *Gazzetta Ufficiale n. 38 del 15 febbraio 2006* - http://www.camera.it/parlam/leggi/06038l.htm - retrieved 2016, October 01.