CJN

Diritto Penale Contemporaneo

RIVISTA TRIMESTRALE

REVISTA TRIMESTRAL DE DERECHO PENAL

A QUARTERLY REVIEW FOR CRIMINAL JUSTICE

Nuove frontiere tecnologiche e sistema penale. Sicurezza informatica, strumenti di repressione e tecniche di prevenzione

IX Corso di formazione interdottorale di Diritto e Procedura penale 'Giuliano Vassalli' per dottorandi e dottori di ricerca

(AIDP Gruppo Italiano, Siracusa International Institute for Criminal Justice and Human Rights – Siracusa, 29 novembre - 1° dicembre 2018)

ISSN 2240-7618

2/2019

Editore Associazione "Progetto giustizia penale", via Altaguardia 1, Milano - c.f. 97792250157
ANNO 2019 - CODICE ISSN 2240-7618 - Registrazione presso il Tribunale di Milano, al n. 554 del 18 novembre 2011.
Impaginazione a cura di Chiara Pavesi

Diritto penale contemporaneo – Rivista trimestrale è un periodico on line ad accesso libero e non ha fine di profitto. Tutte le collaborazioni organizzative ed editoriali sono a titolo gratuito e agli autori non sono imposti costi di elaborazione e pubblicazione. La rivista, registrata presso il Tribunale di Milano, al n. 554 del 18 novembre 2011, è edita attualmente dall'associazione "Progetto giustizia penale", con sede a Milano, ed è pubblicata con la collaborazione scientifica e il supporto dell'Università Commerciale Luigi Bocconi di Milano, dell'Università degli Studi di Milano, dell'Università di Roma Tre, dell'Università LUISS Guido Carli, dell'Universitat de Barcelona e dell'Università Diego Portales di Santiago del Cile.

La rivista pubblica contributi inediti relativi a temi di interesse per le scienze penalistiche a livello internazionale, in lingua italiana, spagnolo, inglese, francese, tedesca e portoghese. Ogni contributo è corredato da un breve abstract in italiano, spagnolo e inglese.

La rivista è classificata dall'ANVUR come rivista scientifica per l'area 12 (scienze giuridiche), di classe A per i settori scientifici G1 (diritto penale) e G2 (diritto processuale penale). È indicizzata in DoGI e DOAJ.

La rivista può essere citata in forma abbreviata con l'acronimo: *DPC-RT*, corredato dall'indicazione dell'anno di edizione e del fascicolo.

La rivista fa proprio il Code of Conduct and Best Practice Guidelines for Journal Editors elaborato dal COPE (Committee on Publication Ethics).

La rivista si conforma alle norme del Regolamento UE 2016/679 in materia di tutela dei dati personali e di uso dei cookies (clicca qui per dettagli).

Ogni contributo proposto per la pubblicazione è preliminarmente esaminato dalla direzione, che verifica l'attinenza con i temi trattati dalla rivista e il rispetto dei requisiti minimi della pubblicazione.

In caso di esito positivo di questa prima valutazione, la direzione invia il contributo in forma anonima a due revisori, individuati secondo criteri di rotazione tra i membri dell'Editorial Advisory Board in relazione alla rispettiva competenza per materia e alle conoscenze linguistiche. I revisori ricevono una scheda di valutazione, da consegnare compilata alla direzione entro il termine da essa indicato. Nel caso di tardiva o mancata consegna della scheda, la direzione si riserva la facoltà di scegliere un nuovo revisore.

La direzione comunica all'autore l'esito della valutazione, garantendo l'anonimato dei revisori. Se entrambe le valutazioni sono positive, il contributo è pubblicato. Se una o entrambe le valutazioni raccomandano modifiche, il contributo è pubblicato previa revisione dell'autore, in base ai commenti ricevuti, e verifica del loro accoglimento da parte della direzione. Il contributo non è pubblicato se uno o entrambi i revisori esprimono parere negativo alla pubblicazione.

La direzione si riserva la facoltà di pubblicare, in casi eccezionali, contributi non previamente sottoposti alla procedura di peer review. Di ciò è data notizia nella prima pagina del contributo, con indicazione delle ragioni relative.

Se desideri proporre una pubblicazione alla nostra rivista, invia una mail a editor.criminaljusticenetwork@gmail.com. I contributi che saranno ritenuti dalla direzione di potenziale interesse per la rivista saranno sottoposti alla procedura di peer review sopra descritta. I contributi proposti alla rivista per la pubblicazione dovranno rispettare i criteri redazionali scaricabili qui.

Diritto penale contemporaneo – Rivista trimestrale es una publicación periódica *on line*, de libre acceso y sin ánimo de lucro. Todas las colaboraciones de carácter organizativo y editorial se realizan gratuitamente y no se imponen a los autores costes de maquetación y publicación.
La Revista, registrada en el Tribunal de Milan, en el n. 554 del 18 de noviembre de 2011, se edita actualmente por la asociación "Progetto giustizia penale", con sede en Milán, y se publica con la colaboración científica y el soporte de la *Università Commerciale Luigi Bocconi* di Milano, la *Università degli Studi di Milano,* la *Università di Roma Tre*, la *Università LUISS Guido Carli*, la *Universitat de Barcelona* y la *Universidad Diego Portales de Santiago de Chile.*
La Revista publica contribuciones inéditas, sobre temas de interés para la ciencia penal a nivel internacional, escritas en lengua italiana, española, inglesa, francesa, alemana o portuguesa. Todas las contribuciones van acompañadas de un breve abstract en italiano, español e inglés.
El lector puede leer, compartir, reproducir, distribuir, imprimir, comunicar a terceros, exponer en público, buscar y señalar mediante enlaces de hipervínculo todos los trabajos publicados en "Diritto penale contemporaneo – Rivista trimestrale", con cualquier medio y formato, para cualquier fin lícito y no comercial, dentro de los límites que permite la licencia *Creative Commons - Attribuzione - Non commerciale 3.0 Italia* (CC BY-NC 3.0 IT) y, en particular, debiendo mantenerse la indicación de la fuente, el logo, el formato gráfico original, así como el autor de la contribución.
La Revista se puede citar de forma abreviada cn el acrónimo *DPC-RT*, indicando el año de edición y el fascículo.
La Revista asume el Code of Conduct and Best Practice Guidelines for Journal Editors elaborado por el COPE (*Comitte on Publication Ethics*).
La Revista cumple lo dispuesto en el Reglamento UE 2016/679 en materia de protección de datos personales (clica aquí para los detalles sobre protectión de la privacy y uso de cookies).
Todas las contribuciones cuya publicación se propone serán examinadas previamente por la Dirección, que verificará la correspondencia con los temas tratados en la Revista y el respeto de los requisitos mínimos para su publicación.
En el caso de que se supere con éxito aquella primera valoración, la Dirección enviará la contribución de forma anónima a dos evaluadores, escogidos entre los miembros del *Editorial Advisory Board*, siguiendo criterios de rotación, de competencia por razón de la materia y atendiendo también al idioma del texto. Los evaluadores recibirán un formulario, que deberán devolver a la Dirección en el plazo indicado. En el caso de que la devolución del formulario se retrasara o no llegara a producirse, la Dirección se reserva la facultad de escoger un nuevo evaluador.
La Dirección comunicará el resultado de la evaluación al autor, garantizando el anonimato de los evaluadores. Si ambas evaluaciones son positivas, la contribución se publicará. Si alguna de las evaluaciones recomienda modificaciones, la contribución se publicará después de que su autor la haya revisado sobre la base de los comentarios recibidos y de que la Dirección haya verificado que tales comentarios han sido atendidos. La contribución no se publicará cuando uno o ambos evaluadores se pronuncien negativamente sobre su publicación.
La Dirección se reserva la facultad de publicar, en casos excepcionales, contribuciones que no hayan sido previamente sometidas a *peer review*. Se informará de ello en la primera página de la contribución, indicando las razones.

Si deseas proponer una publicación en nuestra revista, envía un mail a la dirección editor.criminaljusticenetwork@gmail.com. Las contribuciones que la Dirección considere de potencial interés para la Revista se someterán al proceso de *peer review* descrito arriba. Las contribuciones que se propongan a la Revista para su publicación deberán respetar los criterios de redacción (se pueden descargar aquí).

Diritto penale contemporaneo – Rivista trimestrale is an on-line, open-access, non-profit legal journal. All of the organisational and publishing partnerships are provided free of charge with no author processing fees. The journal, registered with the Court of Milan (n° 554 - 18/11/2011), is currently produced by the association "Progetto giustizia penale", based in Milan and is published with the support of Bocconi University of Milan, the University of Milan, Roma Tre University, the University LUISS Guido Carli, the University of Barcelona and Diego Portales University of Santiago, Chile.

The journal welcomes unpublished papers on topics of interest to the international community of criminal scholars and practitioners in the following languages; Italian, Spanish, English, French, German and Portuguese. Each paper is accompanied by a short abstract in Italian, Spanish and English.

For citation purposes the journal's abbreviated reference format may be used: *DPC-RT,* indicating year of publication and issue.

The journal strictly adheres to the Code of Conduct and Best Practice Guidelines for Journal Editors drawn up by COPE (Committee on Publication Ethics).

The journal complies with the General Data Protection Regulation (EU) 2016/679 (GDPR) (click here for details on protection of privacy and use of cookies).

All articles submitted for publication are first assessed by the Editorial Board to verify pertinence to topics addressed by the journal and to ensure that the publication's minimum standards and format requirements are met.

Should the paper in question be deemed suitable, the Editorial Board, maintaining the anonymity of the author, will send the submission to two reviewers selected in rotation from the Editorial Advisory Board, based on their areas of expertise and linguistic competence. The reviewers are provided with a feedback form to compile and submit back to the editorial board within an established timeframe. If the timeline is not heeded to or if no feedback is submitted, the editorial board reserves the right to choose a new reviewer.

The Editorial Board, whilst guaranteeing the anonymity of the reviewers, will inform the author of the decision on publication. If both evaluations are positive, the paper is published. If one or both of the evaluations recommends changes the paper will be published subsequent to revision by the author based on the comments received and verification by the editorial board. The paper will not be published should one or both of the reviewers provide negative feedback.

In exceptional cases the Editorial Board reserves the right to publish papers that have not undergone the peer review process. This will be noted on the first page of the paper and an explanation provided.

If you wish to submit a paper to our publication please email us at editor.criminaljusticenetwork@gmail.com. All papers considered of interest by the editorial board will be subject to peer review process detailed above. All papers submitted for publication must abide by the editorial guidelines (download here).

Contents

Il diritto penale nel cyberspazio

El derecho penal en el ciberespacio

Criminal Law in Cyberspace

Neutralization Theory: Criminological Cues for Improved Deterrence of Hacker Crimes 1
"Teoria della neutralizzazione": tra prevenzione e repressione del cybercrime
"Teoría de la neutralización": Entre prevención y represión del cibercrimen.
Marcello Sestieri

«Send nudes» Il trattamento penalistico del *sexting* in considerazione dei diritti fondamentali del minore d'età 9
El tratamiento penal del sexting en consideración a los derechos fundamentales de los menores de edad
The Criminalisation of Sexting Involving Underage Victims
Domenico Rosani

Gli effetti dell'automazione sui modelli di responsabilità: il caso delle piattaforme *online* 33
Los efectos de la automatización en los modelos de responsabilidad: el caso de las plataformas online
The Effects of Automation on Imputation Models: the Case of Online Platforms
Beatrice Panattoni

Diritto penale e libertà di espressione in internet

El derecho penal y la libertad de expresión en internet

Criminal Law and Freedom of Expression on the Internet

Istanze di criminalizzazione delle *fake news* al confine tra tutela penale della verità e repressione del dissenso 60
La criminalización de las fake news entre al confín entre tutela penal de la verdad y represión del disenso
Criminalisation of Fake News Between the Protection of Truth and the Suppression of Dissent
Anna Costantini

Il volto dei reati di opinione nel contrasto al terrorismo internazionale al tempo di *Internet* 81
El rostro de los delitos de opinión en la lucha contra el terrorismo internacional en la época de Internet
The Face of Word Crimes in the Fight Against International Terrorism at the Time of the Internet
Paolo Cirillo

Contents

Financial cybercrime

Cibercrimen financiero

Financial Cybercrime

Crowdfounding @ ICOs: esigenze di prevenzione del rischio di commissione di reati nell'era della digital economy 101
Crowdfunding @ ICOs: exigencias de prevención del riesgo de comisión de delitos en la era de la economía digital
Crowdfunding @ ICOs: Commission Risk Prevention Needs of Crimes in the Era of the Digital Economy
Antonietta di Lernia

La tutela penale del segreto commerciale in Italia. Fra esigenze di adeguamento e possibilità di razionalizzazione 112
La tutela penal del secreto comercial en Italia. Entre exigencias de adecuación y posibilidades de racionalización
The Protection of Trade Secret under Italian Criminal Law. Between Needs for Adequacy and Options for Rationalization
Riccardo Ercole Omodei

L'abuso di mercato nell'era delle nuove tecnologie. *Trading* algoritmico e principio di personalità dell'illecito penale 129
Abuso del mercado en la era de las nuevas tecnologías. **Trading** *algorítmico y principio de responsabilidad penal personal*
Market Abuse in the Age of New Technologies. Algorithmic Trading and Principle of Individual Criminal Responsibility
Marta Palmisano

Gli strumenti di prevenzione nazionali ed europei in materia di valute virtuali e riciclaggio 148
Los instrumentos de prevención nacional y europeos en materia de monedas virtuales y lavado de activos
Domestic and European Preventative Instruments Concerning Virtual Currencies and Money Laundering
Cristina Ingrao

Le valute virtuali e gli ontologici rischi di riciclaggio: tecniche di repressione 159
Las monedas virtuales y los ontológicos riesgos de lavado de activos: técnicas de represión.
Virtual currencies and the endemic risk of money laundering: repression techniques
Fabiana Pomes

Contents

La tutela penale della privacy nel cyberspazio

La tutela penal de la privacidad en el ciberespacio

Criminal Law and the Protection of Privacy in Cyberspace

I limiti della tutela penale del trattamento illecito dei dati personali nel mondo digitale 178
Los límites de la tutela penal del tratamiento ilícito de datos personales en el mundo digital
Limits to Criminalization of Unlawful Data Processing in the Digital World
Salvatore Orlando

Il compendio sanzionatorio della nuova disciplina privacy sotto la lente del *ne bis in idem* sovranazionale e della Costituzione 201
El compendio sancionatorio de la nueva regulación de la privacidad bajo la lente del ne bis in idem *internacional y de la Constitución italiana*
The Sanctioning System for Privacy-Related Infringements from the Supranational Ne Bis In Idem *and the Italian Constitution Perspectives*
Ludovica Deaglio

***Eternal Sunshine of the Spotless Crime*. Informazione e oblio nell'epoca dei processi su internet** 212
Eternal Sunshine of the Spotless Crime.
Información y olvido en la época de los procesos de internet
Eternal Sunshine of the Spotless Crime.
The Right to Information and the Right to be Forgotten in Times of Trials by Media
Edoardo Mazzanti

La moltiplicazione dei garanti nel settore della tutela dei dati personali: riflessi penalistici del GDPR 239
La multiplicación de las garantías en el sector de la tutela de los datos personales: Reflexiones penalísticas del GDPR
The Multiplication of Responsibilities in the Personal Data Protection Area: Criminal Law Implications of the GDPR
Gaia Fiorinelli

***Corporate liability e compliance* in the *cyber privacy crime*: il nuovo "modello organizzativo *privacy*"** 251
Responsabilidad corporativa y compliance en el delito de privacidad cibernética: El nuevo "modelo organizativo de privacidad"
Corporate Liability and Compliance in the Cyber Privacy Crime: the New "Privacy Organizational Model"
Valentina Aragona

Contents

Sicurezza informatica, compliance e prevenzione del rischio di reato

Seguridad informática, compliance y prevención del riesgo de delitos

IT Security, Compliance and Crime Prevention

I discorsi d'odio nell'era digitale: quale ruolo per l'internet service provider? 268
Los discursos de odio en la era digital: ¿Cuál es el rol del proveedor de servicios de internet?
Hateful Speech in the Digital Era: Which Role for the ISP?
Valérie Nardi

***Big Data Analytics* e *compliance* anticorruzione** 289
Profili problematici delle attuali prassi applicative e scenari futuri
Análisis de Big Data y compliance anticorrupción
Cuestiones críticas de la práctica actual y escenarios futuros
Big Data Analytics and Anti-corruption Compliance
Critical Issues of Current Practice and Future Scenarios
Emanuele Birritteri

La partita del diritto penale nell'epoca dei *"drone-crimes"* 304
El partido del derecho penal en la era de los "delitos de dron"
The Criminal Law Match in the Era Of "Drone-Crimes"
Carla Cucco

Profili penalistici delle *self-driving cars* 325
Cuestiones de derecho penal en relación a los vehículos de conducción autónoma
Self-driving Cars and Criminal Law
Alberto Cappellini

Gli algoritmi predittivi per la commisurazione della pena. 354
A proposito dell'esperienza statunitense nel c.d. *evidence-based sentencing*
Los algoritmos predictivos para la determinación de la pena. A propósito de la experiencia estadounidense del "evidence-based sentencing"
Predictive Algorithms for Sentencing. The US Experience of the So-Called Evidence-Based Sentencing
Luca D'Agostino

Banche dati, attività informativa e predittività. La garanzia di un diritto penale del fatto. 374
Bases de datos, actividades de información y predictibilidad. La garantía de un derecho penal del hecho
Databases, Information Activities and Prediction. The Safeguard of Fact-related Criminal Law
Pietro Sorbello

Contents

Nuove tecnologie e processo penale

Nuevas tecnologías y proceso penal

New Technologies and Criminal Procedure

Algoritmi predittivi: alcune premesse metodologiche 391
Algoritmos predictivos: algunas premisas metodológicas
The 'multi-faceted' brain of predictive algorithms.
Barbara Occhiuzzi

Algoritmi predittivi e discrezionalità del giudice: una nuova sfida per la giustizia penale 401
Algoritmos predictivos y discrecionalidad del juez: un nuevo desafío para la justicia penal
Predictive Algorithms and Judicial Discretion: a New Challenge for Criminal Justice
Lucia Maldonato

Le nuove indagini tecnologiche e la tutela dei diritti fondamentali. L'esperienza del captatore informatico 417
Las nuevas tecnologías de investigación y la tutela de los derechos fundamentales. La experiencia del software espía
New IT-based Investigations and Protection of Fundamental Rights. The Case of Spy-software
Gaia Caneschi

Il controllo occulto e continuativo come categoria probatoria: premesse teoriche di una sistematizzazione 430
El control oculto y continuado como categoría probatoria: premisas teóricas de una sistematización
The Hidden and Continous Control as Evidentiary Notion: Theoretical Premises for a Systematic Analysis
Fabio Nicolicchia

L'accesso transfrontaliero all'*electronic evidence*, tra esigenze di effettività e tutela dei diritti 439
El acceso transfronterizo a evidencia electrónica, entre exigencias de efectividad y tutela de derechos
Transnational Access to Electronic Evidence Between Effectiveness and the Need to Protect Rights
Veronica Tondi

Contents

L'utilizzo dello *smartphone* alla guida nei delitti di omicidio e lesioni colpose stradali: l'accertamento processuale della colpa attraverso i c.d. *file* di *log*. 456
El uso del smartphone al momento de conducir en los delitos de asesinato y lesiones culposas: la verificación procesal de la culpa a través del archivo de registro
The Usage of Smartphones While Driving and The Road/Traffic-Related Crimes of Manslaughter and Personal Negligence-Based Injuries: the Assessment of Negligence in Court Through the So-Called Log Files.
Giacomo Maria Evaristi

Spunti per una riflessione sul rapporto fra biometria e processo penale 465
Ideas para reflexionar sobre la relación entre biometría y proceso penal
Ideas for a Reflection on the Relationship Between Biometrics and Criminal Trial
Ernestina Sacchetto

Il diritto penale nel cyberspazio

El derecho penal en el ciberespacio

Criminal Law in Cyberspace

Neutralization Theory: Criminological Cues for Improved Deterrence of Hacker Crimes

Teoria della neutralizzazione": tra prevenzione e repressione del cybercrime

"Teoría de la neutralización": Entre prevención y represión del cibercrimen.

Marcello Sestieri
Dottorando di ricerca presso l'Università LUISS "Guido Carli"
msestieri@luiss.it

Cybercrimes, Criminology | Reati informatici, Criminologia | Delitos informáticos, Criminología

Abstracts

Delineating a profile for hackers and for cybercrime in general is a complex task. Yet, identifying a criminological theory capable of encompassing all the various "types" of hackers has become a necessity.
The paper begins with a brief analysis of the three main macro-categories of hackers that have been defined at a scientific level (the so-called "black hat", "gray hat", and "white hat" hackers) and then proceeds to examine the compatibility of neutralization theory with the reasons behind the steep rise in cybercrime.
The said theory – developed to describe the increase in juvenile crime in the US during the 1950s – points out a series of psychological processes that lead criminals to neutralize the moral and emotional counter-thrusts to delinquency. In a modern interpretation, these processes seem like a perfect fit for issues related to cybercrime.
Through this re-proposal of neutralization theory, it becomes clear that a traditional manner of thinking of deterrence fails when it comes to repressing cybercrime, and that a multi-sectoral strategy is now required.

Svolgere un'analisi criminologica in materia di *cybercrime* è attività complessa: del resto, ad essere complessi sono i concetti stessi di criminale informatico (in generale) e di *hacker* (in particolare). Dopo aver accennato alle tre principali macro-categorie di *hackers* (*black hat, grey hat* e *white hat*), si tenterà, dunque, di individuare una teoria criminologica unitaria, in grado di sintetizzare le varie anime di tale categoria delinquenziale. In questo senso, riemergono con sorprendente attualità alcuni studi criminologici sviluppati nel secolo scorso: si allude alla c.d. "teoria della neutralizzazione", che, pur non essendo stata pensata per le tematiche relative al *cybercrime*, appare sovrapponibile a detta *species* criminosa. Secondo questa teoria, esisterebbero una serie di processi psicologici che conducono ad un azzeramento di valori al fine di neutralizzare la controspinta morale alla commissione del reato. Si dimostrerà come un simile procedimento risulti facilitato dalle caratteristiche dei reati informatici, che, dunque, si rivelano fattispecie altamente criminogene. Infine, si segnalerà come gli elementi rafforzativi della desensibilizzazione degli *hackers* riverberino altresì non trascurabili conseguenze sul più ampio tema delle funzioni della pena, depotenziando la tradizionale efficacia generalpreventiva e specialpreventiva della repressione ed imponendo al legislatore una maggiore attenzione verso rimedi preventivi di tipo alternativo.

Delinear un perfil criminológico para hackers y para el cibercrimen en general es una tarea compleja. Sin embargo, desarrollar una teoría criminológica capaz de comprender todos los "tipos" de hackers se ha vuelto una necesidad. El presente trabajo comienza con un breve análisis de las tres principales macro categorías de hackers que han

sido definidas a nivel científico (los así llamados "black hat", "gray hat" y "white hat" hackers). Posteriormente, se procede a analizar la compatibilidad de la teoría de la neutralización con las razones detrás del aumento del cibercrimen. Esta teoría, desarrollada para describir el aumento de la delincuencia juvenil en los Estados Unidos durante la década de 1950, señala una serie de procesos psicológicos que llevan a los criminales a neutralizar la moral y los obstáculos emocionales para delinquir. En base a una moderna interpretación de la teoría de la neutralización, se aprecia claramente que la manera tradicional de concebir la prevención falla cuando se trata de combatir el cibercrimen, evidenciando así la necesidad de una estrategia multisectorial.

Sommario

1. Criminology and cybercrime. – 2. The various facets of the "hacker phenomenon". – 3. The rebirth of neutralization theory. – 3.1. Origins and characteristics. – 3.2. Compatibility with cybercrime. – 4. A new perspective on preventing hacker crimes.

1. Criminology and cybercrime.

Cybercrime is an increasingly widespread phenomenon[1], and unlike the manner in which it is typically perpetrated, its effects do not remain "virtual". Indeed, cybercrime can affect not only the victims' financial situation when it is committed for financial gain, but also their fundamental rights, like privacy and security.

There are multiple factors that can favor the commission of cybercrimes, from both the victim and the offender's perspective: although these factors are certainly relevant in all traditional crimes (*e.g.* the victim's greater or lesser vulnerability, the offender's abilities and personality), when it comes to cybercrime the subjective and psychological aspects becomes surprisingly dominant[2].

Precisely because of this major role played by personal abilities and human interactions in cybercrime[3], legal scholars has extended the applicability of many criminological theories elaborated for "traditional" crimes to it, for the specific purpose of profiling hackers.

The aim of this paper is to analyze the application of one of these criminological theories – the so-called "neutralization theory" – to cybercrime, in order to find criminological cues that could guide both Italian and European legislators towards an improved deterrence strategy *vis-à-vis* this phenomenon.

2. The various facets of the "hacker phenomenon".

Carrying out a criminological analysis of cybercrime is extremely complex, as it is quite difficult to even define the concepts of "cybercrime" and "cybercriminal"[4]. Suffice it to note, for example, that legal scholars have developed a multitude of distinct criminological categories just for hackers[5]. While an exhaustive description of these categories would be too lengthy for the present purposes, some brief references to the three main macro-categories of hackers that have been defined at a scientific level will be useful: these are the so-called "black hat", "gray hat", and "white hat" hackers.

[1] Levi (2017), p. 6, points out that, according to the Office of National Statistics of the United Kingdom, in just over a year – from 2015 to March 2016 – «adults aged 16 over experienced and estimated 3.8 million incidents of fraud, with just over half of these being cyber-related». Furthermore, in Sweden – as showed by the Swedish Crime Survey of 2014 – 44% of frauds involved the Internet, while in The Netherlands, from 2010 to 2012, the cost of "identity frauds" alone was estimated at over 200 million euros.

[2] Leukfeldt (2017), p. 12, talks about a "human factor" to indicate how the offender's skills and the different level of the victim's vulnerability can affect both the choice in "target" and the frequency of the commission of computer crimes; the author defines this the "risk of cybercrime victimization".

[3] Leukfeldt *et al. (*2017), pp. 25-26, identify two main categories of attacks, with four variables depending on the intensity of the contact with the victims: low-tech attacks with a high degree of victim-attacker interaction (*e.g.* the use of e-mails or websites for phishing); low-tech attacks with a low degree of victim-attacker interaction (*e.g.* the acquisition of user credentials with a false entry field); high-tech attacks with a low degree of victim-attacker interaction (*e.g.* malware installed on the victim's computer/phone just with the click on a link); high-tech attacks without victim-attacker interaction (*e.g.* the infection hits the website directly, so that just the simple user's log-in allows the acquisition of all his data).

[4] This difficulty is well illustrated by Viano (2017), p. 3: «there is no universal accepted definition of cybercrime. Different definitions have been put forward by experts, the industry and scholars. Some have been used by various governments. They vary in their degree of specificity and breadth. Regardless of the definition, conceptualizing cybercrime raises several key questions, like where do the criminal acts take place in the real and digital worlds and with the help of which technologies; why are damaging activities undertaken; and who are the actors perpetrating the deviant acts? The "Where" of Criminal Activities, Actors, and Victims».
In addition, Coleman and Golub (2008), p. 267, note that: «there are, then, a wide variety of hacker practices that have been assembled out of a diverse collection of exemplary personalities, institutions, political techniques, critical events, and technologies. These practices are not guided by a singular hacker ethic but are instead rooted in and reveal a number of distinct but interesting genres of ethical practice».

[5] McKenzie (2006), p. 320, explains that the term "hacker" migrated from the university world (being previously connected to electrical engineering inventions) to a totally different category: «as computing became a pervasive force with the rise of the Internet, "hacking" developed a second meaning – it named the process of exploring computer networks. In many cases this was benign. The Internet was a new and not well-understood phenomenon, and hackers in this sense were explorers of this new terrain».

The black hat category is constituted by hackers who use their IT skills on an ongoing basis, with methods that tend to be illegal, in order to achieve a profit; hacking becomes an actual "profession" motivated by personal gain.

The gray hats represent an intermediate category composed of hackers who occasionally commit illegal actions, but without the stability characteristic of the black hats' activities. Typically, their actions are not aimed at personal enrichment but other goals, the main one being to benefit the internet community (*e.g.* to show the flaws in a security system). Despite their non-malicious intent, breaking the law would not be a decisive obstacle for gray hats: in fact, hackers in this category do not see themselves as criminals at all[6].

Finally, white hats are hackers who collaborate with law enforcement agencies, often as external consultants. In other words, they are "members of the security industry hired specifically to find security flaws"[7]. As such, further references in this paper to "hackers" will not include white hats: as their actions are not illegal, no criminological analysis is required for them.

3. The rebirth of neutralization theory.

Given the complexity in profiling hackers (and in delineating cybercrime in general), it would be useful, if not necessary, to identify a criminological theory capable of encompassing all the various "types" in this category of offenders. For this very reason, the most recent legal writings – especially in the US – have re-proposed neutralization theory in an effort to acknowledge the reasons behind the steep rise in cybercrime.

3.1. *Origins and characteristics.*

Neutralization theory was developed to describe the increase in juvenile crime in the US during the 1950s. Yet, in a modern interpretation[8], neutralization theory seems like a perfect fit for issues related to cybercrime.

In particular, according to this theory, there are a series of psychological processes that lead criminals to reset their individual values in order to find justifications for their behavior, with the consequence of neutralizing the moral and emotional counter-thrusts to crimes, which are committed, then, without feeling guilty, essentially in a condition of normality.

Gresham Sykes and David Matza postulated the neutralization theory[9] in 1957. Their starting point was a critique of the prevalent criminological theory at the time, according to which there is a radical opposition between the "dominant" values of society and the values adopted by young people who choose to commit crimes[10].

Sykes and Matza asserted that the focus, rather, should be on the reasons why individuals decide to break rules that they often believe in, and suggested that the answer might be a temporary lapse in the delinquent's values – a lapse which occurs solely to make it (psychologically) possible to behave in a manner which, without the neutralization activity, would never have occurred –.

According to the authors, this interior process manifests itself through five main (alternative) neutralization techniques[11]: the first is "Denial of responsibility", which allows the

[6] For more details on gray hats, see Kirsch (2014), pp. 383-405.
[7] Kirsch (2014), p. 386.
[8] Neutralization theory, as we know it today, is the result of numerous additions and interpolations, which have occurred over the years by various authors. For an in-depth analysis of these integrations, see Costello (2000), pp. 307-329.
Among the mentioned theoretical studies, one must mention Agnew and Peters (1986), p. 81. Particularly, the Authors note that, for an effective application and understanding of the neutralization theory, "two dimensions" must be identified: «the first dimension can be viewed as a predisposing factor toward deviance; the second dimension can be viewed as the situational factor that ignites the deviant act».
[9] Sykes and Matza (1957), pp. 664-670.
[10] Minor (1980), p. 112, notes that: «at least since the 1950s, theoretical explanations of crime and delinquency have been largely polarized into subcultural and anti-subcultural positions, in large part on the basis of whether the value system of delinquents was through to be fundamentally different from or fundamentally similar to that of the larger society. It was in this spirit that Sykes and Matza offered neutralization as theoretical alternatives to subcultural commitment».
[11] To these "original" five techniques, two have been added: Minor (1981), pp. 295-318, elaborated the "Defense of necessity" technique, which allows the rationalization of the criminal intent on the assumption that there are no valid possibilities other than committing crimes; while Klockars (1974) postulated the technique known as the "Metaphor of the ledger", through which one manages to tolerate a bad

offender to divert any self-responsibility, treating his own deviant acts like "accidents" and perceiving himself "as helplessly propelled into new situations".

The second is "Denial of injury", a process by which the offender justifies the crime as not having caused any harm, implicitly denying that their conduct could be considered a "*mala*" (a "wrong") but only "*quia prohibita*" ("because prohibited"). The third, "Denial of the victim", means a desensitization technique that allows offenders to tolerate the harm they cause to victims, who are seen as an enemy or simply absent or unknown.

The fourth technique is "Condemnation of the condemners", or contempt towards the authorities tasked with repressing certain crimes; crimes, in turn, are considered justifiable precisely because those authorities lack legitimation. Lastly, the fifth neutralization technique, "Appeal to higher loyalties", represents the inner reasoning that leads the offender to accept their delinquency based on the belief that they are acting for the good of the social group to which they belong[12].

All these techniques have been successively summarized, reworked, extended and incorporated into different professional and/or social contexts in order to find explanations for various deviant behaviors[13]. Some authors have even posited that the neutralization process may last even after the commission of the crime, for as long as the "reset" in values allows the offender to accept their actions and live with them[14].

3.2. *Compatibility with cybercrime.*

It is interesting to observe how, out of the five, Denial of injury, Denial of the victim and Condemnation of the condemners seem perfectly relatable to cybercrime in general, and to the hacker profile in particular. Indeed, all these psychological processes find clear correspondences in typical hacker conduct.

The gray hats category, for example, appears compatible with the Denial of injury technique: these hackers, while knowingly breaking the law, are still convinced that they are not doing anything wrong, because they perceive their actions as merely formal violations that do not actually cause any damage, and often committed to benefit the internet community (in this case, then, with an "Appeal to higher loyalties" as well).

As for Denial of the victim, one must consider that hackers tend to attack targets perceived as enemies by the internet community (*e.g.* companies that strictly protect copyrights); furthermore, cybercrimes represent the category of offences – perhaps *par excellence* – in which the victim is physically absent or unknown during their commission.

Finally, regarding Condemnation of the condemners, one can point out the obvious, *i.e.* that it is characteristic of the hacker community to despise authorities, which are usually perceived as a mere source of oppression against the opportunities that a "boundless Internet" could otherwise guarantee.

All these considerations (and therefore also the idea of devising an all-encompassing hacker profile through neutralization theory) might appear to be a purely theoretical endeav-

action, and overcome a sense of guilt, because they have always acted properly in the past.

[12] This last technique above all does not require a complete repudiation of the fundamental rules of a legal system, despite the failure to follow them. Particularly, Sykes and Matza (1957), p. 669, describe "the conflict between the claims of friendship and the claims of law".

[13] Polding (2017), p. 64, applies neutralization techniques to companies and highlights a series of interior justifications that can be used to "anesthetize one's values". Through the "appeal to higher loyalties" technique, for example, it becomes «acceptable to lie in a report about who was responsible for a business failure if one is protecting his or her own team».

Barlow *et al.* (2013), p. 146, emphasize the role of the "Denial of the victim" technique in the context of IT policy violations: «employees may choose to share a network password because they rationalize that no one is being injured as a result of their actions. […] By rationalizing their motivations, employees attempt to reduce their guilt or shame for intending to violate IT policies».

For another broad analysis of relations between neutralization theory and IT policy violations, see also Silic *et al.* (2017), pp. 1027-1037.

[14] Minor (1984), p. 996, states that: «the question boils down to this: Which came first, the delinquent act or the belief justifying it? To my mind, the assumption that delinquent acts come before justifying beliefs is the more plausible causal ordering with respect to many of the techniques of neutralizations. It is in fact in many cases difficult to imagine how the boy could subscribe to the belief without having engaged in delinquent acts. But these considerations do not require that we reject such "neutralizing" beliefs as causes of delinquency. On the contrary, since a boy may commit delinquent acts episodically over an extended period of time, there is every reason to believe that neutralizations in some sense resulting from the earlier acts are causes of later acts. In fact, if we reject, as we do here, the idea that the delinquent develops a set of beliefs that positively require delinquent behavior, then the development of a series of neutralizing beliefs is exactly what we mean by the "hardening" process that presumably occurs at some point in a delinquent career».

See also Costello (2000), p. 314.

or. However, this theory has recently resurfaced – at least in the US – precisely because of its relevance in practice, as evidenced by the statistical analyses conducted in the field of hacker profiling.

Indeed, according to estimates published by the Italian "Hacker profile project"[15], almost 60% of professional hackers claim to have started this kind of criminal activity between 10 and 15 years of age. This fact alone could bring us full-circle with neutralization theory, which – as a reminder – was originally postulated to explain an increase in juvenile delinquency. Clearly, the basic psychological processes that this theory describes are particularly impactful on younger individuals, for whom finding alternative justifications to the moral duties imposed by society is quite natural.

Another statistical result that gives an account of how effective the rationalization process is for hackers is the following: 65% of professional hackers stated that they did not even consider the possibility of being convicted because of their criminal activity[16], as if it were completely lawful, or their profession were like any other. These statistics demonstrate the existence of a normalization process which affects the cybercriminal's very awareness that they are committing a crime at all.

4. A new perspective on preventing hacker crimes.

All these reflections should push the criminal justice system towards alternative models of contrasting the hacker phenomenon. In fact, what emerges from this re-proposal of neutralization theory is that the standard or traditional manner of thinking of deterrence fails when it comes to repressing cybercrime.

Indeed, on the basis of the "eternal"[17] topic of the "multi-purpose" nature of punishment[18] – split between general deterrence[19] and special deterrence[20] – it becomes clear that the deterrent effect of punishment is scarce when it comes to cybercrime, considering that 65% of professional hackers do not even consider punishment on the assumption that, given the characteristics of cybercrime and cyberspace[21], they will never be caught by national authorities. Moreover, at a special deterrence level, it is likewise obvious that being sentenced for actions that the (cyber)offender does not even recognize as a crime might produce an effect opposite to their desired rehabilitation.

All the above considerations lead to the conclusion that, in order to effectively combat the occurrence and expansion of this type of crime, the criminal justice system should reject a merely repression-oriented perspective. As evidenced by the aforementioned statistics, simply extending traditional criminal justice enforcement to cybercrime would be completely inadequate as a deterrence method. In fact, if 59% of hackers start hacking between 10 and 15 years of age, what use could longer prison terms or new provisions in criminal codes ever have?

It follows that a multi-sectoral strategy seems to be necessity when it comes to curbing the rise in cybercrime. The most effective way to achieve this rather ambitious goal, then, should include direct action on young people's education, showing them the risks of hacking

[15] Chiesa and Ciappi (2007), pp. 84-85, point out that the cases in which the offender starts hacking after the age of twenty are very rare: only 4% of hackers began a criminal activity between 26 and 30 years of age, while just 1% did so after 40.
[16] Chiesa and Ciappi (2007), pp. 205-207.
[17] So described by Vassalli (1991), 619-656. The Author points out that, beyond deterrence purposes, it is undeniable that the primary function of punishment is to "reaffirm" the existence of the violated right, in order to "offset" the negative effects of the offender's conduct. Such reaffirmation "is separate from the punishment inflicted on the offender, so much so that it exists irrespective of whether the punishment is actually carried out".
[18] On the multi-faceted nature of criminal sanctions, see Mezzetti (2017), p. 711, but also Pulitanò (2017), p. 49.
[19] General deterrence is based on the idea that the threat of punishment can distract people from criminal behavior. Through "social disapproval", which creates an internal counter-thrust with a deterrent effect, general deterrence is able to create a "habit contrary to crime". This first aim of the criminal justice system can be viewed as the punishment's "effectiveness as a deterrent", or its dissuasive potential.
[20] Special deterrence, instead, works on an individual level: the criminal sanction tries to prevent the offender from "returning to crime", operating in a perspective of re-socialization. This purpose appears to be closely related to the rehabilitative purpose of the criminal sanction, required by Article 27(3) of the Italian Constitution.
Indeed, according to the Italian Constitutional Court, Judgment no. 236/2016, proportionality and rehabilitative purposes should support the criminal sanction at every stage: from when it is conceived in the abstract, to when it is applied in reality. With regard to this judgment, see Viganò (2017), pp. 61-66.
[21] Flor (2012), p. 1, describes a "de-timing of the activities" in order to emphasize how IT products are simultaneously opportunities for social development but also new potential forms of crime.

and explaining the criminal offences that it constitutes. Only by identifying the educational messages best suited to the age group in which this phenomenon is prevalently rooted can the criminal justice system truly be successful in preventing the birth of new cybercriminals.

Still, since justice and necessity are at the basis of the criminal sanctions system[22], legislators can never simply forego punishing perpetrators of cybercrimes; at the same time, however, legislators can no longer simply rely on typical criminal justice methods and provisions to fulfill their duty in preventing this phenomenon.

To conclude, in this day and age, intervening during the early stages of criminal behavior seems to be essential in order to curtail the process of normalization of cybercrime[23].

References

Agnew Robert and Peters Ardith (1986): "The Techniques of Neutralization: An Analysis of Predisposing and Situational Factors", *Criminal Justice and Behavior*, 13, pp. 81-97

Barlow Jordan, Warkentin Merril, Ormond Dustin and Dennis Alan (2013): "Don't Make Excuses! Discouraging Neutralization to Reduce IT Policy Violation", *Computer & Security*, 39, pp. 145-159

Chiesa Raoul and Ciappi Silvio (2007): *Profilo Hacker. La scienza del Criminal Profiling applicata al mondo dell'hacking* (Milano, Apogeo); Coleman Gabriella and Golub Alex (2008): "Hacker practice. Moral Genres and the Cultural Articulation of Liberalism", *Anthropological Theory*, 8, pp. 255-277

Costello Barbara (2000): "Techniques of Neutralization and Self-esteem: a Critical Test of Social Control and Neutralization Theory", *Deviant Behavior*, 21, pp. 307-329; Flor Roberto (2012): "Lotta alla "criminalità informatica" e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di internet", *Diritto penale contemporaneo*, pp. 1-13

Kirsch Cassandra (2014): "The Gray Hacker: Reconciling Cyberspace Reality and the Law", *Northern Kentucky Law Review*, 41, pp. 383-405

Klockars Carl (1974): *The Professional Fence* (New York, Free Press); Leukfeldt Rutger (2017): *The Human Factor in Cybercrime and Cybersecurity* (The Hague, Eleven International Publishing)

Leukfeldt Rutger, Kleemans Edward and Stol Wouter (2017): "A Typology of Cybercriminal Networks: from Low-tech All-rounders to High Tech Specialists", *Crime, Law and Social Change*, 67, pp. 21-37

Levi Michael (2017): "Assessing the Trends, Scale and Nature of Economic Cybercrimes: Overview and Issues", *Crime, Law and Social Change*, 67, pp. 3-20; McKenzie Wark (2006): "Hackers", *Theory, Culture & Society*, 23, pp. 320-322

Mezzetti Enrico (2017): *Diritto penale. Casi e materiali*, 2ª ed., (Bologna, Zanichelli); Minor William (1980): "The Neutralization of Criminal Offence", *Criminology*, 18, pp. 103-120

Minor William (1981): "Techniques of Neutralization: a Reconceptualization and Empirical Examination", *Journal of Research in Crime and Delinquency*, 18, pp. 295-318; Minor William (1984): "Neutralization as a Hardening Process: Considerations in the Modeling of

[22] Vassalli (1961), pp. 303-306.

[23] In particular, Barlow *et al.* (2013), p. 146, point out that: «in addition to reacting to security policy violations by applying sanctions to employees who exhibit deviant behavior, organizations must also use proactive measures to deter and prevent such abuse, including the implementation of security education, training and awareness programs. […] Improved training techniques and other communication that focus on reducing rationalization behaviors may be the key in helping employees understand that policy-breaking is neither common nor acceptable. Because neutralization techniques often are stronger than sanctions in influencing intention to violate, researchers and practitioners should combat neutralization techniques directly through persuasive communication to employees, including security training programs».

Change", *Social Forces*, 62, pp. 995-1019

Polding Brian (2017): "The Extension of Neutralization Theory to Business Ethics", *Journal of Leadership Studies*, 11, pp. 63-65

Pulitanò Domenico (2017): "La misura delle pene, fra discrezionalità politica e vincoli costituzionali", *Diritto penale contemporaneo - Rivista trimestrale*, 2, pp. 48-60

Silic Mario, Barlow Jordan and Back Andrea (2017): "A New Perspective on Neutralization and Deterrence: Predicting Shadow IT Usage", *Information & Management*, 54, pp. 1027-1037

Sykes Gresham and Matza David (1957): "Techniques of Neutralization: A Theory of Delinquency", *American Sociological Review*, 22, pp. 664-670

Vassalli Giuliano (1961): "Funzioni e insufficienze della pena", *Rivista italiana di diritto e procedura penale*, pp. 297-346

Vassalli Giuliano (1991): "La pena in Italia, oggi", in *Studi in memoria di Pietro Nuvolone*, Vol. I, (Milano, Giuffrè), pp. 619-656

Viano Emilio (2017): *Cybercrime, Organized Crime and Social Responses*, (Cham, Springer)

Viganò Francesco (2017): "Un'importante pronuncia della Consulta sulla proporzionalità della pena", *Diritto penale contemporaneo - Rivista trimestrale*, 2, pp. 61-66.

Diritto Penale Contemporaneo

RIVISTA TRIMESTRALE

REVISTA TRIMESTRAL DE DERECHO PENAL

A QUARTERLY REVIEW FOR CRIMINAL JUSTICE

http://dpc-rivista-trimestrale.criminaljusticenetwork.eu