Quasi-Property on Customer Information: Trade Secrets and Consumer Rights in the Age of Big Personal Data

by

Gianclaudio Malgieri*

I. INTRODUCTION

In the world of Big Data[1], intellectual capital of businesses is more and more grounded in commodification of "consumers' identities"[2].

New technologies, and in particular artificial intelligences, have extremely developed the value and potentialities of customer information for companies, especially by means of "data mining" and open data: forecasts, behaviour evaluations (based on cognitive phycology and behavioural economics)[3], studies on life expectancy, personalized marketing plan, automated profiling, creditworthiness, etc.[4]

Such an intellectual work on customer information (that we can call "intellectual privacy") is highly valuable and needs specific attention. Traditionally, trade secret is the intellectual property right used to protect these data.[5] Actually, customer information is personal data of individuals and as such it concerns also data protection law. Moreover, data protection rights and duties are more and more pervasive and based on a proprietary approach.[6]

Therefore, "consumer identities" are the object of two intangible monopolies: intellectual property of businesses and data protection rights of consumers.

In this intersection some interests are common to companies and individuals (data secrecy, reasonable measures to protect secrecy, personal data integrity, correctness of personal data),

* Gianclaudio Malgieri is a Research Assistant at Sant'Anna School of Advanced Studies

[1] See O. TENE, J. POLONETSKY, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 Nw.K. Tech. & Intell. Prop. 239, 2013, 257

[2] N. ELKIN-KOREN & N. WEINSTOCK NETANEIL, *The Commodification of Information*, The Hague, 2002; L. LESSIG, *Privacy as Property*, 69 *Social Research, 2002,* 247-270.

[3] See, e.g., J. METHA, *Economics in Competition and Consumer Policy*, University of East Anglia, ESRC Centre for Competition Policy, UEA Repository, 2013.

[4] See Art. 15(1) of 95/46/EC and art. 4(3a) of the Proposed General Data Protection Regulation, which refers to "*economic situation, location, health, personal preferences, reliability or behaviour*". See F. PASQUALE, *The Black Box Society*, *The Secret Algorithms That Control Money and Information*, Cambridge, MA, 2015.

[5] B. REDDIX-SMALLS, *Credit Scoring and Trade Secrecy: An Algorithmic Quagmire or How the Lack of Transparency in Complex Financial Models Scuttled the Finance Market*, 12 U.C. DAVIS BUS. L.J. 87, 117-18 (2011).

[6] J.M. VICTOR, *The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy*, Yale Law Journal, 123, 2, (2013), 266.

while others are controversial (right to data access, right to data portability, right "to be forgotten"[7]).

Indeed, it is not just a coincidence that two parallel reforms have been proposed in the European Union in these two fields: the "General Data Protection Regulation"[8] and the first Directive on Trade Secrets[9].

In fact, in the EU the actual legal framework about the management of data is fragmented and problematic: several member states have no trade secret protection[10]; balancing rules between data protection and economic interests are quite unclear (*infra)*; the scholarly debate (in the EU and between the EU and the US) about this intersection is still at an early stage.[11]

In this context, several interests are in conflict and several theoretical problems require a solution.

First of all, it is necessary to determine "ownership" of immaterial goods related to consumers and to understand whether allocating economic rights on personal data to consumers is efficient and consistent with the European Digital Single Market strategy[12] and respectful of personality rights of individuals.[13]

Secondly, several rules in personal data protection framework are problematic in terms of trade secrecy (right to access), competition law (right to data portability) [14], intellectual property law (right to be forgotten).[15]

---

[7] As regards balancing interests under the Draft Data Protection Regulation see G. SARTOR, *The right to be forgotten: balancing interests in the flux of time*, *Int J Law Info Tech*, first published online November 25, 2015.

[8] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011).

[9] Proposal for a Directive of the European Parliament and of the Council on the Protection of Undisclosed Know-how and Business Information (Trade Secrets) against their unlawful acquisition, use and disclosure /*COM/2013/0813 final-2013/0402 (COD).

[10] See, in general, BAKER & MCKENZIE, *Study on Trade Secretsand Confidential Business Information in the Internal Market, Final Study prepared for European Commission*, April 2013 (available at: http://ec.europa.eu/internal_market/iprenforcement/docs/trade-secrets/130711_final- study_en.pdf).

[11] See P. SCHWARTZ, D. SOLOVE, *Reconciling Personal Information in the United States and European Union*, 102 Cal. L. Rev. (2014), 877; V. MAYER-SCHONBERGER*, Beyond Privacy, beyond Rights - Toward a Systems Theory of Information Governance*, 98 Cal. L. Rev. 2010, 1853.

[12] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *A Digital Single Market Strategy for Europe* COM(2015) 192 final.

[13] N. PURTOVA, *The Illusion of Personal Data as No One's Property*, Law, Innovation and Technology, vol. 7, n. 1, 2015, 83. See also D. SOLOVE, *The Digital Person*, New York, 2004, 76-80; P. SCHWARTZ, *Property, Privacy, and Personal Data*, 117 Harv. L. Rev. 2004, 2055; L. LESSIG, *Code and Other Laws of Cyberspace*, Basic Books, New York, N. Y., 1999, 142 ff.

[14] Article 18 of Proposed General Data Protection Regulation.

[15] European Data Protection Supervisor, *Opinion on the Data Protection Reform Package*, 7 March 2012, § 150-152.

In general, there is an uncertain "grey area" in which determining "default entitlement" of data is particularly challenging: it is the case of the intellectual output of customer data, all information created by (automated[16] or human) processing of raw data; in other words, it is the case of the final product of Big Data analytics and in general all customer data which are just forecasted, statistically predicted, obtained by the original combination of probabilistic data, meta-data and raw data related to customers.[17]

To find a solution to this grey area "default entitement" issue[18], we should first analyse balancing rules in the EU legal system.

Balancing rules in the EU law proves to be schizophrenic. In fact, on the one hand, a prevalence of trade secrets on data protection rights is proposed[19]; on the other hand, a prevalence of data protection rights on trade secrets is affirmed as well[20].

Moreover, in the global digital market the legal differences between the EU and the US approach to consumer personality rights[21] (and in particular to personal data protection) is a great problem in terms of international trade and the development of global economics. [22]

II. WHY TRADE SECRETS AND NOT DATABASES

The dynamism of trade secret well meets the exigencies of the "information" market.[23]

Even though apparently "databases", in the form of "sui generis" rights related to copyright and regulated in Europe at Article 7 of 96/9/EC, are the best form of protection for collection of customer personal data[24], the statutory protection of "database"[25] in Europe proves to be incomplete and inappropriate to data collection and data processing: it is difficult for

---

[16] As regards automated creation of original databases see G. SARTOR, *Cognitive Automata and the Law: electronic contracting and the intentionality of software agents*, in Artificial intelligence and the law, 17(4), 283.

[17] F. PASQUALE, *The Black Box Society*, supra at n. 3.

[18] This issue is even more complicate when the agents are software agents, see G. SARTOR, *Cognitive Automata and the Law*, EUI Working Papers, Law No. 2006/35, 30 and 44.

[19] Recital 41 of 95/46/EC and Recital 51 of the Proposed General Data Protection Regulation.

[20] Recital 28 of the Proposed Directive on Trade Secrets.

[21] V. MAYER-SCHONBERGER, *Beyond Privacy, Beyond Rights*, supra at n. 11, 1853; P. SCHWARTZ, D. SOLOVE, *Reconciling Personal Information in the US and EU*, supra at note 11, 877.

[22] E. FAHEY, D. CURTIN, *A Transatlantic Community of Law. Legal Perspectives on the Relationship between the EU and US Legal Orders*, Cambridge, 2014.

[23] B.T. ATKINS, *Trading Secrets In The Information Age*, cit., 1194, which affirms that trade secret law *"is the most flexible area of intellectual property law*".

[24] Diritto Industriale

[25] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the Legal Protection of Databases, *OJ* 1996 L 077/20. See C. PRINS, *Property and Privacy: European Perspectives and the Commodification of our Identity*, Information Law Series, Vol. 16, 2006, 229-230.

companies to demonstrate specific financial investments to process such list when the processing of data is automated, the genetic non-secrecy of statutory protection of databases is not suitable in terms of competition strategies, the exclusive protection of the forms of expression more than of the content reveals how databases were not conceived for trade exigencies.[26]

Moreover, databases tend to consider data as "units", atoms, concretely collectable in a static way. This view of personal data is anachronistic in the age of data driven economy: Big Data analytics, data mining, Internet of things and artificial intelligences contribute to make personal data as an "ecosystem", more than single static units.[27]

To cope with this dynamic "ecosystem", the most suitable intellectual property right is trade secret, as a fluid and versatile protection of immaterial assets of businesses. In fact, trade secrets, as they protect "confidentiality", are based exactly on total secrecy, protection of the content, economic value *per se*.[28]

III. THE INTERSECTION OF TWO LEGAL FRAMEWORKS

The main legislative frameworks implied in this debate are data protection laws and trade secret laws. They are both apparently "new" laws in the western legal experience, as they reflect the challenge to protect information in the new economy. However, they are also really fragmented and heterogeneous, from a supranational perspective.

After all, it is not a mere coincidence the parallel statutory revolution that is affecting these two subjects in the European Union. In fact, the 20-year-old European directive 95/46/EC on data protection[29] is going to be totally reformed by a General Data Protection Regulation[30], in discussion from 2012 by the European institutions.

---

[26] See I. LLOYD, *Legal Aspects Of The Information Society*, London, 2000, 177-191. J. LIPTON, *Protecting Valuable Commercial Information in the Digital Age: Law, Policy and Practice*, 6 J. Tech. L. & Pol'y 2, 2001, §1; P. DAL POGGETTO, *La protezione giuridica delle banche dati mediante il diritto d'autore ed il diritto sui generis,* in *Informatica e diritto*, 1997, 159.

[27] PURTOVA, *The Illusion of Personal Data as No One's Property* ,2015, supra at note 13.

[28] P.SAMUELSON, *Information as Property: Do Ruckelshaus And Carpenter Signal A Changing Direction In Intellectual Property Law?*, 1989 Cath.U.L. Rev., 365

[29] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the processing of personal data and on the free movement of such data, *OJ* L 281 , 23/11/1995, 31-50.

[30] European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)).

At the same time, the European Union for the first time is going to approve a directive on trade secrets[31], a subject before left to the single national laws.[32]

It is clear that this strong exigency to harmonize and centralize (as regards data protection from a directive to a regulation; as regards trade secrets from heterogeneous national laws to a directive) derives from the fluidity of "data economy" in the global digital world and stimulates a comparison with the main interlocutor of the global trade: the United States.[33]

Unlike European law, the Us law on trade secrets is already "centralized" since 1979 by the Uniform Trade Secret Act[34], which allows each state to implement it with a national law, and so the effect would be very similar to the proposed European directive: a common base with different laws reflecting each territorial industrial peculiarity.[35]

At the same time, unlike European law, the US law on data protection is neither uniform, nor divided in national statutes, but fragmented per area and based on self-regulation. This situation has stimulated scholars and case law to use trade secret law to try to better protect customer databases, and this is very interesting for our purposes.[36]

However, this issue is likely to be analyzed from an inter-institutional perspective: the proximity to the concept of "property", the relevance of human rights at issue and the social dangerousness of information espionage, in fact, require the parallel intervention of civil law and criminal law.[37]

IV. RISKS AND DAMAGES: THE DIMENSION OF THE PROBLEM

The importance for legal science to address these issues is revealed by the incredible growth of unfair practices aiming at misappropriating trade secrets, such as theft, unauthorised

---

[31] Proposal for a Directive Of The European Parliament and of the Council on the Protection of Undisclosed Know-how and Business Information (Trade Secrets) against their unlawful acquisition, use and disclosure /* COM/2013/0813 final - 2013/0402 (COD).

[32] See, in general, BAKER & MCKENZIE, *Study on Trade Secrets and Confidential Business Information in the Internal Market, Final Study prepared for European Commission*, April 2013 (available at: http://ec.europa.eu/internal_market/iprenforcement/docs/trade-secrets/130711_final-study_en.pdf).

[33] See *Proposal for a Directive on the Protection of Undisclosed Know-how and Business Information*, cit., *Explanatory Memorandum*, *Context of the Proposal*, §1.

[34] Uniform Trade Secrets Act (UTSA), published by the Uniform Law Commission (ULC) in 1979 and amended in 1985.

[35] See B.T. ATKINS, *Trading Secrets In The Information Age*, cit., 1195.

[36] S.K. SANDEEN, *Relative Privacy: What Privacy Advocates Can Learn From Trade Secret Law,* 2006 MICH. ST. L. REV. 667; J. McNEALY, *Who Owns Your Friends?: Phonedog V. Kravitz And Business Claims Of Trade Secret in Social Media Information*, 39 Rutgers Computer & Tech. L.J. 30, [2013].

[37] See *Proposal for a Directive on Trade Secrets*, cit., *Impact Assessement*, § 2.2.

copying, economic espionage, breach of confidentiality requirements. A phenomenon obviously amplified by globalisation, longer supply chains, increased use of information and communication technology.[38]

Just to understand the dimension of the problem, it is useful to quote some figures: according to unofficial estimates of the US Defense Department, the industrial espionage and misappropriation of intellectual property and sensitive data cause damages of about a trillion dollars a year.[39] Furthermore, the International Center for Strategic Studies in Washington estimated that cybercrime and cyber espionage cost the US economy 100 billion dollars a year, and the global economy about 300 billion dollars[40]. From 2011 to 2014 cyber-espionage has registered an increase of 146% in the world[41] and, for example, an increase of 200% in Italy.[42]

Regarding data breaches, over 22,960,000 cases of data breaches involving personally identifiable information were reported in the US through July of 2011, and in 2009 through 2010, over 230,900,000 cases of personal data breaches were reported[43].

What is even more interesting is that the 22% (the second biggest cause) of data breaches confirmed around the world were perpetrated by cyber-espionage[44], so revealing the strong link between personal data protection and trade secrets protection.

V. THEORETICAL IMPLICATIONS

This technical debate implies even a bigger theoretic revaluation of the "information" as a good, also considering all implications on competition law, intellectual property and data protection law[45].

---

[38] See *Proposal for a Directive on Trade Secrets*, cit, recital (3).

[39] P.PASSERI, Cybercrime: Risks for the Economy and Enterprises at the EU and Italian Level, UNICRI, 2014, 52.

[40] *Ibidem*, 53.

[41] *Ibidem*, 49.

[42] See CLUISIT, *Rapporto Cluisit 2015 sulla sicurezza ICT in Italia*, Milan, 2015.

[43] Sec. 2 (11), S.1995 - *Personal Data Protection and Breach Accountability Act* of 2014.

[44] Verizon Enterprise, *2014 Data Breach Investigations Report,* Executive Summary, 3 (available at http://www.verizonenterprise.com/DBIR/2014/reports/rp_dbir-2014-executive-summary_en_xg.pdf).

[45] In the US the precise collocation of "trade secret law" has implied several problems, in fact, modern trade secret law has been described "*as a combination of contract, tort, agency, trust, and equity law supplementing the common-law right of invention*". B.T. ATKINS, *Trading Secrets In The Information Age: Can Trade Secret Law Survive The Internet?*, 1996 U. Ill. L. Rev. 1151; See also A.H. SEIDEL, *What The General Practitioner Should Know About Trade Secrets And Employment Agreements*, 2d Ed., Philadephia, 1984, § 1.01.

However, our issue reveals the necessity to renew some traditional legal categories: the concept of "secret" may revolutionize the traditional legal approach to the "information" good.[46]

The blurred difference between "secrecy" and "privacy"[47] involves the difference between information property (or quasi-property[48]) and personal human rights.[49]

Two opposite options may solve this theoretical conflict: the "commodification" of personal data[50] or the reconsideration of "personality" of legal persons.

A compromise between these two extremes would be necessary to cope with this challenge: the overcoming of traditional barriers and a complex shared management of secret data.[51]

VI. DEFINITION AND REQUIREMENT OF TRADE SECRET… IN THE INFORMATION AGE

To start, it is fundamental to understand the right meaning of "trade secrets" and of "personal data" in our legislative framework.

Many expressions are used to generically define "trade secrets": confidential documents, secret information, commercial secrets, sensitive economic data, protected contents, etc.[52] In the global Information Society it is extremely important to have clear definitions of trade secrets.

In Europe, each jurisdiction has adopted heterogeneous eligibility standards for information to be qualified as trade secrets.[53] In fact, as the Explanatory Memorandum of the Proposal for a Directive reveals, "*trade secret-based competitive advantages are at risk (reduced*

---

[46] See P.SAMUELSON, *Information as Property: cit.*, 365, where only trade secrets are considered "property" (though immaterial) because of the role of "secrecy" on information.

[47] See *infra,* Section 1, final § 4.

[48] D.G. BAIRD, *Common Law Intellectual Property and the Legacy of International News Service v. Associated Press, 50 U.CHI. L. REV. 411 (1983); ID., Misappropriation, and Preemption: Constitutional and Statutory Limits of State Law Protection,* 1983 SUP. CT. REV. 509

[49] See P.SAMUELSON, *Information as Property, cit.*

[50] N. ELKIN-KOREN & N. WEINSTOCK NETANEIL, *The Commodification of Information*, The HAGUE, 2002; L. LESSIG, *Privacy as Property*, 69 *Social Research* 247-270 (2002);

[51] See *Infra, Conclusion: "A multi-level management of personal data".*

[52] P. WACHSMANN, *Le droit au secret de la vie privée*, in F. SUDRE (dir.), *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme*, Bruylant, 2005, p. 120.

[53] BAKER & MCKENZIE, *Study on Trade Secrets and Confidential Business Information in the Internal Market, Final Study prepared for European Commission*, April 2013 (available at: http://ec.europa.eu/internal_market/iprenforcement/docs/trade-secrets/130711_final-study_en.pdf)., p.4-5.

competitiveness): the fragmented legal protection within the EU does not guarantee a comparable scope of protection and level of redress within the Internal Market".[54]

Unfortunately, in the matter of data secrets, international agreements are vague and general, as this subject is considered really susceptible to industrial and economic differences between countries, and so a "minimum approach" has been preferred.[55]

The first and unique international definition of trade secrets comes from the *Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPs Agreement).* Article 39, section 2, in fact, defines trade secrets as "*information* [that] *is secret, in the sense that it is not (…) generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question*; [that] *has commercial value because it is secret and has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret*".

In Europe, despite the above mentioned heterogeneity, a common core of requirements for trade secrets among member state laws can be found in: a) technical or commercial value of the information related to the business; b) secrecy in the sense of a not general notoriety or easy accessibility; c) economic value consisting of conferring a competitive advantage to its owner; and d) reasonable steps taken to keep it secret.[56]

As regards the Proposed European Directive on trade secrets, it defines at Article 2, paragraph 1 the meaning of "trade secret", which is the exact reproduction of Article 39(2) TRIPs, with its lack of detail. For example if the requirement of "reasonable steps to protect secrecy", as vague as it is, can be appropriate in an international agreement, it shows an unacceptable degree of detail in a European framework of harmonization.[57]

The probable result will be presumably that each member state will implement a different "trade secret" eligibility test on confidential information[58], with the risk that some information will be totally protected in some parts of EU and will be unprotected in some other parts. The information which most risks to suffer this heterogeneity is customer data,

---

[54] Proposed Directive on Trade Secret, supra, *Explanatory Memorandum*, §2.2

[55] See, similarly, why in the USA the discipline of trade secrets was addressed at state level, Trading secret, 1195. See also, in general, C.R.J. PACE, *The Case for a Federal Trade Secret Act*, 8 Harv.Jour. Law & Thech., 427 (1995).

[56] BAKER & MCKENZIE, *Study on Trade Secrets*, supra, p. 4-5.

[57] See R. KNAAK, A. KUR, R.M. HILTY, *Comments of the Max Planck Institute for Innovation and Competition of 3 June 2014 on the Proposa l of the European Commission for a Directive on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) Against Their Unlawful Acquisition, Use and Disclosure of 28 November 2013, COM(2013) 813 Final*, Munich, 2014, § 19.

[58] *Id.*

which traditionally are not unanimously considered fulfilling trade secret requirements.[59]

An interesting model that should be considered with respect to this issue is US law. In fact, United States, apart from being the major trading partner of Europe, has a long tradition in establishing legal rules protecting trade secrets, and has also implemented the above-cited TRIPs Agreement.[60]

Indeed, in the USA the legal framework is clearer: the Restatement of torts of 1939 offers six specific factors for courts to consider when determining whether a supposed trade secret is legally protectable: "(1) the extent to which the information is known outside of business; (2) the extent to which it is known by employees and others involved in business; (3) the extent of measures taken to guard the secrecy of the information; (4) the value of the information to the business and competitors; (5) the amount of effort or money expended by the business in developing the information; (6) the ease or difficulty with which the information could be properly acquired or duplicated by others".[61]

However, the American discipline has undergone a long development[62] which culminated in the approval of the Uniform Trade Secrets Act in 1979, emended in 1985 and now adopted by 47 of the American States. UTSA proposed a general supranational approach to trade secrets. It defines trade secrets as "*information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy*".[63]

The common denominator is undoubtedly represented by: information with competitive value (based on commercial or technical values, acquired with more or less financial investment) based on secrecy, which is actual and protected by reasonable measures.

V. WHEN TRADE SECRETS ARE PERSONAL DATA

It is not difficult to understand the strong link between data secrets and data protection.

---

[59] See B. VAN WYK, *We're Friends, Right? Client List Misappropriation and Online Social Networking in the Workplace*, 11 Vand. J. Ent. & Tech. L. 743, 757, *passim*.

[60] See*, WTO TRIPS Implementation*, http://www.iipa.com/trips.html (last visited April, 26th 2015).

[61] Restatement of Torts 757 cmt. b (1939).

[62] See, in general, S.K. SANDEEN, *Relative Privacy: What Privacy Advocates Can Learn From Trade Secret Law,* 2006 MICH. ST. L. REV. 667.

[63] Unif. Trade Secrets Act 1(4), 14 U.L.A. 438 (1985).

Personal data protectable under European law are defined by Article 2(a), directive 95/46/EC[64] as "*any information relating to an identified or identifiable natural person (data subject*)" where "an identifiable person is "one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".

It is clear that commercial secrets may consist of personal data,[65] for instance of customers, suppliers and employees[66]: the content of negotiations with clients, the identity of those clients (customer lists), their commercial profiles, etc., are all extremely valuable elements for businesses and are all considered "confidential".[67]

In fact, customer lists are now one of the most precious assets for businesses which operate in the global market[68]: of course there are businesses for which customers' personal data are fundamental, like advertising companies, insurers, banks, etc.[69] However, in general, consumers' information constitutes a necessary intangible asset for every kind of business, because every company has clients, an advertising plan (often related to customer profiling operations), etc.[70] Actually, a great market of personal data has arisen: the so called "personal data trade"[71].

Taking all the above into account, the centrality of the following issues appears extremely clear. Indeed, it is worth investigating both (1) in which terms the definitions of trade secrets can include the definition of personal information databases, and (2) which are the conditions and restraints enabling to consider personal data of consumers as trade secrets according to the various legal frameworks of trade secret protection summarized above.

1. "Customer Information" in the Different Definitions of Trade Secret

---

[64] And by Article 4(2) of the Proposed General Data Protection Regulation.

[65] Consumer data would not be personal data only if anonymized by businesses. This phenomenon is much more important with "Big Data", see in general Article 29 Data Protection Working Party, *Opinion 05/2014 on Anonymisation Techniques*, Adopted on 10 April 2014, 0829/14/EN, WP216.

[66] BAKER & MCKENZIE, *Study on Trade Secrets and Confidential Business Information in the Internal Market, Final Study prepared for European Commission*, p. 5: "commercial secrets may consist of customer and supplier lists"; see also WIPO's definition "What is a trade secret", available at http://www.wipo.int/sme/en/ip_business/trade_secrets/trade_secrets.htm .

[67] F. MOULIERE, *Secret des affaires et vie privée*, Recueil Dalloz, 2012, p. 573

[68] See X.-T.N. NGUYEN, *Collateralizing privacy, 78 Tul. L. Rev. 553,* [2004], which critically analyses the phenomenon of businesses, which "collateralize" customer information in secured transactions as corporate asset.

[69] B. VAN WYK, *We're friends, right?,* supra, 760.

[70] *Ibid.*, 761.

[71] See, *e.g.*, F. ROCHELANDET, *Economie des données personnelles et de la vie privée*, Paris, 2010, passim; A.E. LITTMANN, *The Technology Split in Customer List Interpretation*, 69 U. Chi. L. Rev. 1901, (2002), p. 1912-1914.

In dealing with the first question we can generally include the concept of personal data collections in the concept of valuable, secret and protected information provided for by art. 39,2 TRIPs and echoed by article 2,1(a) of the *Proposal for a trade secret directive*, although some clarifications will be necessary on the notions "secrecy" and "economic value" *(infra).*

Recital (1) of the Proposal confirms this approach when stating that trade secrets companies tend to protect several business and research innovation management tools, which cover "*a diversified range of information, (…) such as information on customers and suppliers, business plans or market research and strategies*".[72]

Annex 21 of the impact assessment, which discusses the impact on fundamental rights, is even more explicit when it affirms: "*information kept as trade secrets (such as list of clients/ customers; internal datasets containing research data or other) may include personal data*".[73]

In the USA, as well and although UTSA definition of trade secrets refers generally to "information, including (…) compilation", the Third Restatement on Unfair Competition, at chapter 4, topic 2, §39 clarifies that a trade secret "*can also relate to other[74] aspects of business operations such as pricing and marketing techniques or the identity and requirements of customers*". Already the First Restatement of Torts was clear about this point. In fact, comment "b" of section 757, clarified that "Trade secrets may be (…) a list of customers". Moreover, even if trade secret "generally relates to the production of goods (…) it may, however, relate to the sale of goods or to other operations in the business, such as a code for determining discounts, rebates or other concessions in a price list or catalogue, or a list of specialized customers, or a method of bookkeeping or other office management".

With reference to this difference between trade secrets related to "production" and trade secrets related to "sale", the definition in the European Proposal may be controversial. In fact, Article 2(4) defines "infringing goods" as *goods whose design, quality, manufacturing process or marketing significantly benefits from trade secrets unlawfully acquired, used or disclosed*. Actually, it has been noted that *marketing a good* is not connected with the *use* of a trade secret. It rather constitutes a consequent act of production, but is not as such the result of a trade secret use. If the notion of "marketing benefiting from unlawful use of a trade secret"

---

[72] See, with the same words, Proposed Directive on Trade Secrets, cit., Memory Explanandum, §1.

[73] *Id., Impact assessment*, Annex 21, 254. See, the criticisms of P. HUSTINX, *Opinion of the European Data Protection Supervisor on the proposal for a directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure*, Bruxelles, 12 March 2014l §11.

[74] "Other" compared to "*formula, pattern, compilation of data, computer program, device, method, technique, process, or other form or embodiment of economically valuable information (…) composition or design of a product, a method of manufacture, or the know-how necessary to perform a particular operation or service*".

should cover also marketing campaigns based on customer lists that were unlawfully acquired, it would by far exceed the legitimate purpose of the provision if the products marketed in that manner were classified as infringing.[75]

However, this issue does not contradict, and to the contrary reaffirms, the general interrelation between consumer data and trade secrets.

2. Conditions under which Consumers' Data are Trade Secrets… in the Information Age

However, although generically the definition of customers' personal data can be included in trade secret definition, the problem is to understand under which conditions the law protects a customer database as an intangible asset (or as an Intellectual Property right[76]) of businesses.

As in the European Union there is not a uniform jurisprudence about trade secret protection, to answer this more difficult question, we can begin with analyzing how American courts have applied the 6-steps test on trade secrets to customer lists.

In other words, the test requires to determine whether *a)* personal information contained in the list is secret in the market and as much as possible among the employees[77]; *b)* the information contained in the list is of value[78]; *c)* the "owner" has taken "reasonable steps" or "precautions" to protect the secrecy of the list[79]; *d)* the "owner" has expended resources in developing the list[80] (whose information is therefore difficult to be acquired and/or duplicated).[81]

However, the diffusion of Information and Communication Technologies and the expansion of social networks over the Internet[82] complicate the application of the test . for example to secrecy of personal data, to the efforts to acquire and duplicate them and to the concrete measures of protection. Furthermore, all points enucleated above are deeply interrelated to

[75] See R. KNAAK, A. KUR, R.M. HILTY, *Comments of the Max Planck Institute for Innovation and Competition*, cit., §22.

[76] About the relation between Trade secrets and Intellectual Property Rights see in general M. PASTORE, *La tutela del segreto industrial nel sistema dei diritti di privative,* in G. RESTA, *Diritti esclusivi e nuovi beni immateriali*, Turin, 2011, 271 ss.

[77] Points 1 and 2 of Restatement of torts, art. 39, 2(a) TRIPs and art. 2(1)(a) of Proposal.

[78] Point 4 of Restatement, art. 39, 2(b) TRIPS, art. 2(1)(b) of Proposal.

[79] Point 3 of Restatement of Torts, cit., art. 39, 2(c) TRIPs, and art. 2,1(c) of Proposal.

[80] Point 5 and 6 of Restatement.

[81] For the application of this test to client lists, see B. VAN WYK, *We're Friends, Right? Client List Misappropriation and Online Social Networking in the Workplace*, 11 Vand. J. Ent. & Tech. L. 743, 757.

[82] *Ibid.*

each other: data value depends on their actual secrecy (which depends also on reasonable precautions taken) and on the efforts to acquire/duplicate those data.

a) With reference to *actual secrecy*, courts have produced some general rules to help applying the test.[83] Consumer information is secret not only if it is unavailable on public registers[84], but also on social networks "lists of friends"[85]. According to the Fifth Circuit, the general rule is that a customers list "of readily ascertainable names and addresses will not be protected as a trade secret"[86]. Instead, detailed information contained in a customer list, such as type and color of products purchased by the customer, dates of purchase, amounts of purchase, and certain names and addresses, are not known or available to the public.[87] What differentiate a protectable detailed client list from a non-protectable list of mere names is the large amounts of accompanying information in the list that "*could be compiled only at considerable expense*".[88]

Therefore, it is necessary that consumer information is "ancillary" beyond a simple series of names and addresses[89], but also not public on the Internet. The problem is that Social Networks contain many commercially valuable data and allow users the option of making their profiles open to the public. This free disclosure of personal data makes those data non-protectable as trade secrets: only where profiles are specifically made private, so that only contacts authorized by users to view their profiles can see them, the information in those private profiles should be considered actually secret and, thus, should be given trade secret protection.[90]

---

[83] *See* Metallurgical Indus. Inc. v. Fourtek, Inc., 790 F.2d 1195 (5th Cir. 1986).

[84] See *Infra, Section 1, § 3*.

[85] B. VAN WYK, *We're Friends Right?,* cit., 754.

[86] *Zoecon Indus. v. American Stockman Tag Co.,* 713 F.2d 1174, 1179 (5th Cir. 1983); see also *Gaal v. BASF Wyandotte Corp.*, 533 S.W.2d 152, 155 (Tex. Civ. App. 1976); *Burbank Grease Servs. v. Sokolowski*, 693 N.W.2d 89 (Wis. Ct. App. 2005), review granted 700 N.W.2d 271 (Wis. 2005) (finding a list of potential customers readily ascertainable from the Internet, trade associations, and by asking customers whom to contact)

[87] *Zoecon Indus.*, 713 F.2d at 1179.

[88] See *Mercer v. C.A. Roberts Co*., 570 F.2d 1232 (5th Cir. 1978) (finding that a "mere list of customers," including information readily ascertainable from other sources, was not protectable as a trade secret).

[89] See, e.g., *Amoco Prod. Co. v. Laird*, 622 N.E.2d 912, 918-19 (Ind. 1993) (emphasizing the importance of ease of proper acquisition in granting trade secret protection to plaintiff).

[90] See I. BYRNSIDE, *Six Clicks of Separation: The Legal Ramifications of Employers Using Social Networking Sites to Research Applicants*, 10 Vand. J. Ent. & Tech. L. 445, 473; *Smith v. Dravo Corp*., 203 F.2d 369, 371-72 (7th Cir. 1953) (protecting information as secret even where owner revealed the secret to others); see also *Rockwell Graphic Sys., Inc. v. DEV Indus., Inc*., 925 F.2d 174, 176 (7th Cir. 1991) (finding actual secrecy even where thousands of drawings were in the hands of unauthorized users, in large part because of the reasonable efforts taken to maintain the secrecy of the drawings).

It is interesting that, in this field, "privacy concerns" of users[91] allow an economic "proprietary" protection[92] of those data for businesses: the common ground is secrecy. Furthermore, this phenomenon highlights an interesting link between *privacy by design* on the Internet and reasonable precautions to protect trade secrets.[93]

b) In analyzing the value of customer lists as trade secrets, a premise on the economic value of trade secret evaluation in the EU is necessary. In fact, applicable national rules do not always take into account the intangible value of trade secrets, which makes it difficult to demonstrate the actual profits lost or the unjust enrichment of the infringer where no market value can be established for the information in question. Only few Member States allow for the application of abstract rules on the calculation of damages based on the reasonable royalty or fee which could have been due had a license for the use of the trade secret existed.[94]

However, US courts accepted economic value of consumer information even before Internet was such a wide phenomenon[95]. Furthermore, courts along with statutory interventions and scholarly writings,[96] explicitly consider customer lists as corporate property that is both valuable and freely alienable[97]. This is confirmed also by several bankruptcy cases[98], where courts focused on the correct valuation of customer lists[99].

---

[91] B. VAN WYK, *We're Friends Right?,* supra,758.

[92] See M. PASTORE, *La tutela del segreto industrial nel sistema dei diritti di privative,* in G. RESTA, *Diritti esclusivi e nuovi beni immateriali*, supra., P. SAMUELSON, *Privacy as Information,* supra.

[93] See *infra*, Section 2, 14.1.

[94] See recital (6) of the Proposal for a European Directive on Trade Secrets.

[95] See e.g. *Moss, Adams & Co. v. Shilling, 179 Cal. App. 3d 124, 129 (1986).*

[96] See, for e.g., *Internal Revenue Code,* 26 USC § 936(h)(3)(B)(v) (1994) (defining "intangible property" from which income can be derived as including a "customer list"). See also S.L. KROLESKI and D.R. RANT, *Use of Customer Lists: A Unified Code Is the Solution*, 15 Westchester Bus J 189, 209: "*All lists should be considered assets of the employer, as evidenced by the fact that, when a business is sold, monies are paid for such assets*".

[97] For e.g., in *Miller v Ortman*, 235 Ind 641, 136 NE2d 17 (1956), the Indiana Supreme Court held that a customer list was a part of "the good will of a business" and so freely alienable and owned by the corporation. Other more recent cases [*In re Uniservices*, 517 F2d 492 (7th Cir 1975); *Frank v Hadesman and Frank Inc*., 83 F3d 158, 161 (7th Cir 1996)] added that the fact that the company's "customer information constitutes protectable property is underscored by the assignment thereto of independent market values".

[98] *In re Andrews*, 80 F3d 906 (4th Cir 1996), involved a bankrupt debtor who had sold his customer list, as part of a pre-petition sale, for approximately $ 1 million and the validity of the sale was not questioned.
See also, *In re Lifschultz Fast Freight*, 132 F3d 339, 352 n 12 (7th Cir 1997); *In re Roman Cleanser Co*, 802 F2d 207, 208 (6th Cir 1986) which have permitted debtors to grant security interests in customer lists, thereby acknowledging the debtors' property interest in those lists and allowing the sale of the customer lists in the normal course of business.

[99] See criticisms of A.E. LITTMANN, *The Technology Split in Customer List Interpretation*, 69 U. Chi. L. Rev. 1901, (2002), 1912 ss.

The economic value of online contact lists is clear for many businesses, since conducting business often involves identifying the people who might be customers.[100] Depending on the particular industry, information may be more or less valuable.[101]

However, it's obvious that, in the Information Society, customer (or "user") data have acquired great value. There is a wide market of personal data on the Internet[102], based on the complex intersection between marketing businesses and Internet service providers (especially Social Network Services and online stores). In fact, personal data on the web are generally called "currency" of the Information Society,[103] also because their exploitation is the economic justification for the gratuitousness of most Internet services.[104]

A confirmation of this "value" comes from several economic studies about privacy and digital identity: businesses can now even calculate economic value of each digital identity.[105]

c) "Reasonable precautions" represent a very interesting requirement. In fact, all definitions of trade secrets require "steps"[106], "measures"[107], "efforts"[108] or "precautions" to keep information secret. However, regarding "customer information" these measures have a peculiar value because of their strong link with European data protection law. A specific paragraph will be dedicated to the comparison between "reasonable" protection of trade secret under US law and compulsory measures of protection of personal data under Article 17(1) of European directive on Data Protection and Article 30 of the Proposed Data Protection Regulation[109]. However, for the moment, it suffices to highlight that, in the European Union, there is a statutory duty to protect customer data processing by "appropriate measures", and so this trade secret requirement is always met by client lists.

---

[100] B. VAN WYK, *We're Friends Right?,* supra, 760.

[101] *Ibid.*, 761.

[102] See, e.g., F. ROCHELANDET, *Economie des données personnelles et de la vie privée*, Paris, 2010, 88-114.

[103] See, in general, S. LEMAN-LANGLOIS, *Privacy As Currency: Crime, Information, and Control in Cyberspace*, in *Technocrime: Technology, Crime and Social Control*, Devon, 2008, 112.

[104] Trans Europe Expert, "*Le défis de la Révolution Numérique: Protection des Données Personnelles et Gratuité des Usages*", supra.

[105] Boston Consulting Group, *The Value of Our Digital Identity*, Liberty Global Policy Series, 2012 *passim*. (available at http://www.libertyglobal.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf last visited April, 26th 2015).

[106] Art. 2(1,b) of the Proposal and Art. 39, (2)(c) TRIPs.

[107] Restatement of torts, sec. 757, comment b. "Definition of Trade Secret", point 3.

[108] Uniform Trade Secret Act, Sec.1.(4)(ii).

[109] See *Infra*, Section 2, § 14.1

d) Financial efforts to develop client lists, and the related difficulty to create or duplicate customer information represent the only requirement which is not in Article 39(2) TRIPS nor in art. 2 of the Proposal, but only in the Restatement of torts[110]. At the same time, it is the requirement which has been influenced more by the advent of the Digital Age: less resources to manage lists of data, zero efforts to duplicate and reproduce them.

Nevertheless, "financial efforts" requirement is strongly related to actual secrecy (see point a, above) and value of secrets (see point b, above). In fact (sub-a) US case law has stated that what qualifies client lists as trade secrets is the large amounts of ancillary information in the list that "*could be compiled only at considerable expense*".[111] Moreover, (sub-b) if customer data are generally sold and bought, the "third party" business who buys customer data fulfill the requirement of financial efforts[112]. However, the work of marketing, profiling, etc., requires many economic resources (e.g. the salary of appointed employees).[113] Therefore, even this requirement is almost ever fulfilled.

3. Data Protection Law Protects Customer Information Even if they are not Trade Secret? The Problem of "Publicly Available" Personal Information

It is clear that some personal consumer data cannot be included in the protected category of trade secrets: although requirements *b)* and *c)* are generally fulfilled[114], actual secrecy and economic resources represent a problematic point, especially in the Information Society Age.[115]

Therefore, personal data which are made public on Social Network Services or which are mere lists of names do not fulfill neither the requirements of actual secrecy (*a*) nor economic resources to acquire them (*d*).[116]

---

[110] Restatement of torts, sec. 757, comment b., point 5.

[111] See *Zeocon Indus. v. American Stockman Tag* Co., 713 F.2d 1174, 1179 (5th Cir. 1983).

[112] F. ROCHELANDET, *Economie des données personnelles et de la vie privée*, supra.

[113] B. VAN WYK, *We're friends, right?*, supra.

[114] See *supra*.

[115] See B.T. ATKINS, *Trading secret in Information society*, cit., A.E. LITTMANN, *The Technology Split in Customer List Interpretation*, 69 U. Chi. L. Rev. 1901, (2002), 1907.

[116] B. VAN WYK, *We're friends, right?,* cit., 763.

It is now important to understand whether these "non-trade-secret" consumer data are at least protectable under European Data Protection law, otherwise we will be able to affirm a strong coincidence between protectable trade secrets and protectable personal data.

Personal data publicly available are addressed in two different ways by European data protection law: data available in public registers (e.g., administrative acts, telephone directory, etc.) and data made public by the data subject.

European data protection law considers these kinds of data in four distinct cases:

1) There is a general exception to the prohibition of processing "*sensitive data"* if "the processing relates to [personal] data which are manifestly made public by the data subject" at Article 8,1(e) of directive 95/46 and Article 9,1(e) GDPS.
2) Another exception can be found with regard to the adequacy conditions of *data transfers* to non-EU countries if personal data derive from public registers[117]. In particular, Article 44,1(g) of the Proposal for a GDPS affirms that "*in the absence of an adequacy decision pursuant to Article 41* (decision of the Commission*) or of appropriate safeguards pursuant to Article 42* (e.g., binding corporate rules, standard data protection clauses, etc.), *a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that*: (…) *(g) the transfer is made from a register on data which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest* (…).

   A similar rule can be found at Article 26,1(f) of current 46/95 data protection directive.[118]
3) One last interesting exemption based on the circumstance of publicly available data has been recently proposed among the amendments of European Parliament to the Proposed General Data Protection Regulation. In particular, Article 14 provides the general obligation to inform data subject about a processing of data related to him. Paragraph (3) originally provided that if the personal data are not collected from the data subject the controller shall also inform the data subject "from which source the personal data originate". Now paragraph (3) has been amended so that "*if personal data originate from publicly available sources, a general indication may be given".* Therefore, even if for a little

[117] See R. PERRAY, "*Informatique: données à caractère personnel; formalité préalables à la mise en oevre d'un traitement de données à caractère personnel*", in *LexisNexis Juris Classeur,* fasc. 247-30, p.135.

[118] For a general review about implementation of this rule under national laws, see T.J. KOBUS III, G.S. ZEBALLOS, *BakerHostetler's 2015 International Compendium of Data Privacy Laws*, on www.bakerlaw.com (available at http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/International-Compendium-of-Data-Privacy-Laws.pdf, last visited April, 26th, 2015).

scope, the fact that some data are publicly available lightens the obligations of controller (and therefore also the protection of data subject's rights).

4) Finally, Italian data protection statute (Article 24, 1(c), d.lgs. 196/2003) provides that consent is not required if the processing of personal data relates to data taken from publicly available registers or records.[119]

   Italian scholars have accepted a wider definition of "publicly available registers or records". In fact, it has been specified that, according to a correct interpretation of the provision, also all personal data that can be found on Internet websites can be included in the scope of Article 24, 1 (c).[120]

   However, the Italian Data Protection Authority has specified that not all publicly available data can be considered in the scope of Article 24, 1(c): it has explicitly excluded, in fact, data which are public on the Internet because the reference to "registers and records" should be circumscribed to "institutional" registers only.[121] However, it has been specified that although publicly available on the Internet, personal data (in particular email addresses) cannot be indiscriminately processed[122], because it is necessary to respect the purpose for which those data were made public on the Internet. Just for the use of those data in compliance with that purpose the consent of data subject is not required.[123]

   However, all general principles and rules of data protection must be anyway applied to these data (except for the consent).[124]

   There are no similar rules in any other European Member States, but only for example in Mexico[125] and in Canada, where paragraphs 7 (1)(*d*) and (2)(*c.1*) of Personal Information Protection and Electronic Documents Act (*PIPEDA*) provide an exception for collection

[119] What is interesting is that letter d) of the same article specifies that also data relating to economic activities that are processed in compliance with the legislation in force as applying to business and *industrial secrecy* are excepted from the consent requirement. See *infra.*

[120] G. COMANDÈ, *Commento agli articoli 11 e 12 della legge 675/96,* in *La tutela dei dati personali, Commentario alla legge 675/96,* cit., 120. M.A. GARZIA, *Sub Art. 24, 1° (c),* in *La Protezione dei Dati Personali*, supra, 558.

[121] Garante per la Protezione dei Dati Personali, decision 11 January 2001, in *Bollettino*, 16, 39.

[122] Garante per la Protezione dei Dati Personali, Decision of 28 May 2002, Bagnara c. Consulenza Imm. Maggio; Decision of 29 May 2003, in *Relazione del Garante per la Protezione dei Dati Personali,* 2003, 91.

[123] *Ibid*.

[124] Garante per la Protezione dei Dati Personali, decision of 11 January 2001, in *Bollettino*, 16, 39. See similarly Parere Garante, 1/2000, Relazione, 2000, supra, 285.

[125] Federal Law on the Protection of Personal Data held by Private Parties of July 6, 2010 (Ley Federal de Protección de Datos Personales en Posesión de Particulares). See, T.J. KOBUS III, G.S. ZEBALLOS, *BakerHostetler's 2015 International Compendium of Data Privacy Laws,* supra, 121.

and use of personal information "*without knowledge or consent*" if data are publicly available.[126]

In conclusion, although European data protection law protects also "non secret" personal data, all exceptions reported above demonstrate how this protection is weaker when data are publicly known than when they are secret (regarding data transfer, sensitive information processing, and in some cases even the "consent" requirement in data processing).

However, even if consumer information were not protectable as a trade secret, it would be always protected by means of "data protection" law.

In fact, the European Data Protection framework protects data subjects (and data controllers) from "personal data breach"[127], defined generally as "*the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".* Therefore, in the European Union, even if some customer databases were not definable as trade secrets (because, *e.g*., not totally secret), a misappropriation of them would be anyway unlawful and protected by law.

The only difference is for companies: when customer data are publicly available (e.g. in social networks) they cannot receive any intellectual property protection on their customer databases.

VI. CONCLUSION AND FURTHER STIMULUS: A SHARED QUASI-PROPERTY ON DATA

Proved this strong intersection, we should now understand how to balance right and duties of companies in this conflict between intangible monopolies.

Actually, balancing rules in the EU framework are quite unclear and the only possible solution is an approach on a case-by-case basis.[128]

The only possible solution would be a technical multi-level management of data. It would be interesting to qualify this form of cooperation in terms of joint-controlling, as the Proposed General Data Regulation encourages and better regulates this form of collaboration between individuals (data subjects) and companies (data controllers) at Article 24.

---

[126] For the definition and interpretation of "publicly available", see *Regulations Specifying Publicly Available Information* (SOR/2001-7).

[127] See Article 17(1) of 95/46/EC directive and the explicit definition of data breach at 4 (9) of the Proposed General Data Protection Regulation.

[128] See G. MALGIERI, *Trade Secrets v. Personal Data: Possible Solution for Balancing Rights*, in International Data Privacy Law, 2016, first published online 29 January 2016.

This debate can offer an interesting stimulus to the issue of propertization of personal data. Several scholars, in fact, tried to define and analyze the "default entitlement" of personal data and the "de facto" property of personal data.[129]

Actually, if we consider that trade secrets are considered in common law as "quasi-property rights"[130] and that the idea of quasi property leads to a contextual right, much used to protect competition strategies[131] we can try to apply this legal concept to personal data.

In fact, quasi-property was conceived specifically to cope with the unwillingness to "propertize" objects related to intimacy of human beings (corpse)[132] and so to cope with the unwillingness to "commodify" identity-related goods. Later, this concept developed in terms of propertization on intangible goods[133]

In conclusion, we propose to adopt a shared-management of "quasi-property" on personal data, so that intellectual property rights of companies can reconcile with data protection rights of individuals, in a way both respectful of business relations both consistent with the theory of "shared privacy" and of multi-stakeholder management of the Information Society.[134]

---

[129] N. PURTOVA, *The illusion of property,* supra at note 2013; J.M. VICTOR, *The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy*, supra at note 6.

[130] *S. BALGANESH, Quasi-Property: Like, but not Quite Property, 160 U..Penn.Law Rev. 2012, 1889*

[131] *Ibidm*.

[132] Ibidem.

[133] The recent case O'Grady v. Superior Court, 44 Cal. Rptr. 3d 72, 112 (Ct. App. 2006) referred to "trade secrets" as "quasy-property". Also International News Service v. Associated Press 248 U.S. 215 (1918) referred to "information" as "quasi-property". See generally D.G. BAIRD, *Common Law Intellectual Property and the Legacy of International News Service v. Associated Press, 50 U. CHI. L. REV. 411 (1983);* ID*., Misappropriation, and Preemption: Constitutional and Statutory Limits of State Law Protection,* 1983 SUP. CT. REV. 509. See the criticisms of P.SAMUELSON, *Information as Property*, 1989 Cath.U.L. Rev., 365; C.T. GRAVES, *Trade Secret as Property: Theory and Consequences, ,* 15 J. Intell. Prop. 39 2007-2008.

[134] *See* M.I. COOMBS, *Shared Privacy and the Fourth Amendment, or the Rights of Relationships*, 75 CAL. L. REV. 1593 (1987); K.J. STRANDBURG, *Privacy, Rationality, and Temptation: A Theory of Willpower Norms*, 57 RUTGERS L. REV. 1235, 1298 (2005).