

**PATRICIA PECK GARRIDO PINHEIRO**

**O DIREITO INTERNACIONAL DA PROPRIEDADE INTELECTUAL  
APLICADO À INTELIGÊNCIA ARTIFICIAL**

**TESE DE DOUTORADO**

**ORIENTADORA: PROFA. ASSOCIADA DRA. MARISTELA BASSO**

**UNIVERSIDADE DE SÃO PAULO**

**FACULDADE DE DIREITO**

**São Paulo-SP**

**2018**

**PATRICIA PECK GARRIDO PINHEIRO**

**O DIREITO INTERNACIONAL DA PROPRIEDADE INTELECTUAL  
APLICADO À INTELIGÊNCIA ARTIFICIAL**

Tese de Doutorado, apresentada à Banca Examinadora do Programa de Pós-Graduação em Direito, da Faculdade de Direito da Universidade de São Paulo, como exigência parcial para a obtenção do título de Doutora em Direito, na área de concentração Direito Internacional e Comparado, sob a orientação da Professora Associada Dra. Maristela Basso.

**UNIVERSIDADE DE SÃO PAULO**

**FACULDADE DE DIREITO**

**São Paulo-SP**

**2018**

Autorizo a reprodução e divulgação total ou parcial deste trabalho, por qualquer meio convencional ou eletrônico, para fins de estudo e pesquisa, desde que citada a fonte.

### CATALOGAÇÃO DA PUBLICAÇÃO

Pinheiro, Patricia Peck Garrido

O direito internacional da propriedade intelectual aplicado à inteligência artificial / Patricia Peck Garrido Pinheiro. -- São Paulo: USP / Faculdade de Direito, 2018.

316f.

Orientadora: Professora Associada Dra. Maristela Basso.

Tese (Doutorado), Universidade de São Paulo, USP, Programa de Pós-Graduação em Direito, Direito Internacional e Comparado, 2018.

1. Bases de dados. 2. Propriedade intelectual. 3. Privacidade. 4. Internet das Coisas. 5. Inteligência Artificial. 6. Direito de acesso aos dados. 7. Tratado internacional. 8. Contrato. 9. Arbitragem. I. Basso, Maristela. II. Título.

CDU

Nome: PINHEIRO, Patricia Peck Garrido

Título: O direito internacional da propriedade intelectual aplicado à inteligência artificial

Tese de Doutorado, apresentada à Banca Examinadora do Programa de Pós-Graduação em Direito, da Faculdade de Direito da Universidade de São Paulo, como exigência parcial para a obtenção do título de Doutora em Direito, na área de concentração Direito Internacional e Comparado, sob a orientação da Professora Associada Dra. Maristela Basso.

Aprovada em:

Banca Examinadora

Prof. Dr. \_\_\_\_\_

Instituição: \_\_\_\_\_

Julgamento: \_\_\_\_\_

Profa. Dra. \_\_\_\_\_

Instituição: \_\_\_\_\_

Julgamento: \_\_\_\_\_

Prof. Dr. \_\_\_\_\_

Instituição: \_\_\_\_\_

Julgamento: \_\_\_\_\_

Prof. Dr. \_\_\_\_\_

Instituição: \_\_\_\_\_

Julgamento: \_\_\_\_\_

Prof. Dr. \_\_\_\_\_

Instituição: \_\_\_\_\_

Julgamento: \_\_\_\_\_

## **DEDICATÓRIA**

Uma das coisas mais importantes na jornada de um escritor é ter um verdadeiro companheiro que saiba compreender a necessária solidão exigida para o despertar mais profundo do momento criativo. Pois, o tempo é uma das moedas mais importantes para se concretizar o sonho de um doutoramento, a amarga rotina que exige uma disciplina mais que espartana e um desassossego permanente para fazer brotar as ideias do fundo da alma atormentada do criador. Por isso, a inovação nunca é fruto de uma única mente, mas de todo um contexto familiar, de toda uma história de vida. Sendo assim, dedico esta realização ao meu marido, Romulo Pinheiro, minha alma gêmea de corpo espiritual e intelectual, pelo incentivo permanente para que eu realizasse este importante projeto para a minha vida acadêmica e profissional.

## AGRADECIMENTOS

À minha querida orientadora Dra. Maristela Basso, por ter me aceitado desde o início como sua aluna orientanda, por todo seu apoio durante o processo de definição do tema, por suas aulas fantásticas e inspiradoras que me fizeram ficar mais fascinada pelo Direito Internacional Privado e pela Propriedade Intelectual, pelo carinho com que sempre recebeu todas as minhas dúvidas e limitações, por ter me acompanhado nesta árdua jornada contribuindo para meu crescimento intelectual, e por ser esta pessoa tão inspirada e inspiradora cujo trabalho profissional e acadêmico admiro muito.

Às Instituições de Ensino e de Pesquisa estrangeiras que me aceitaram para que eu pudesse promover a análise de Direito Comparado tão necessária para o aprofundamento do tema objeto do presente estudo, em especial ao Max Planck Institute, de Hamburgo e de Munique, nas pessoas dos professores Jürgen Basedow e Reto Hilty, respectivamente, e à Universidade de Columbia, de Nova Iorque, na pessoa da Professora Jane Ginsburg, por terem me acolhido com muita hospitalidade e por terem me recebido como pesquisadora visitante para realização de meus estudos, o que permitiu que eu pudesse ter acesso a um conteúdo mais atualizado sobre o tema objeto da tese, além do acesso aos professores que sempre estiveram disponíveis para me ajudar durante toda a minha estadia.

À todos os professores da Universidade de São Paulo com os quais eu tive aula nas disciplinas que cursei para cumprir os créditos do doutorado, com os quais eu pude trocar muitas ideias e experiências nestes últimos anos, tendo aprendido muito com cada um deles. Nossos debates me ajudaram muito no despertar do tema e desabrochar da tese, em especial, cito, em ordem alfabética: Prof. Antônio Carlos Morato, Prof. Alberto do Amaral Júnior, Prof. Balmes Vega Garcia, Profa. Cláudia Perrone-Moisés, Profa. Cristiane Lucena, Prof. Eduardo Tomasevinius Filho, Profa. Flávia Piovesa, Prof. Fernando Campos Scaff, Prof. Geraldo Miniuci Ferreira Júnior, Prof. Gustavo Ferraz de Campos Monaco, Prof. Ignácio Maria Povedo Velasco, Prof. José Augusto Fontoura Costa, Profa. Juliana Krueger Pela, Prof. Marco Fábio Morsello, Profa. Maria Cristina da Silva Carmignani, Prof. Newton Silveira, Prof. Rodrigo Sampaio, Profa. Silmara Chinellato, Profa. Sheila C. Neder Cerezetti, Prof. Umberto Celli Júnior e Prof. Wagner Menezes.

Aos professores que aceitaram, gentilmente, participar da pesquisa empírica realizada, visto que o tema é extremamente atual e, por isso, nem tudo está já escrito em livros e em artigos publicados, demandando a coleta das visões e das opiniões acerca do tema e das tendências para possíveis soluções diretamente dos especialistas e pesquisadores sobre o assunto, nas mais diversas localidades, quer seja por agendamento de entrevistas presenciais, via conferência ou via resposta ao questionário enviado por *e-mail*: Prof. Albert Gidari (Universidade de Stanford), Prof. Alexandre Dias Pereira (Universidade de Coimbra), Profa. Ann Bartow (Universidade de New Hampshire), Prof. Chris Reed (Queen Mary Universidade de Londres), Profa. Daphne Keller (Universidade de Stanford), Prof. Dario Moura Vicente (Universidade de Lisboa), Prof. Eike Hosemann (Max Planck Institute), Prof. Gerald Splindler (Universidade de Gottingen), Profa. Gloria Gonzales Fuster (Universidade

de Bruxelas), Profa. Jacqueline Lipton (Universidade de Akron), Prof. Jan Luttrinhaus (Max Planck Institute), Prof. Jan Schmidt (Max Planck Institute), Prof. Jeremy Malcolm (Electronic Frontier Foundation - EFF), Prof. Josef Drexl (Max Planck Institute Munich), Profa. June Besek (Universidade de Columbia), Prof. Luis Filipe Antunes (Universidade do Porto), Profa. Nathália Mazonetto (Universidade de São Paulo), Prof. Nicholas Hernanz (do Partido The Greens – Parlamento Europeu), Prof. Rafael Ferraz Vazques (World Intellectual Property Organization - WIPO), Prof. Reinhard Zimmermann (Max Planck Institute), Prof. Remédio Marques (Universidade de Coimbra), Reto M. Hilty (Max Planck Institute), Prof. Rolf Weber (Universidade de Zurich), Profa. Roya Ghafele (Universidade de Oxford), Profa. Valentina Moscon (Max Planck Institute), Prof. Wolf Meier-Ewert (World Trade Organization - WTO).

À minha fiel e incansável correspondente internacional na Alemanha, que desempenhou um papel primordial de pesquisa, Dra. Mellany Prawda, que por mais de um ano me apoiou nos estudos profundos da propriedade intelectual e seus desdobramentos transnacionais, tendo me acompanhando na realização do trabalho de campo na Europa, além da busca por informações preciosas que muito enriqueceram o projeto e sem as quais eu não teria sozinho alcançado o mesmo resultado.

A minha estudiosa pesquisadora assistente Larissa Lotufo por sua valiosa contribuição para o aprofundamento das referências doutrinárias e busca de conteúdos relevantes para embasar os questionamentos e os debates na busca da resposta à pergunta principal formulada pela tese no tocante a quem cabe a propriedade intelectual das bases de dados digitais e do conhecimento resultante aprendido por máquina em um contexto em que a sociedade avança para a aplicação cada vez maior da inteligência artificial.

À toda a minha equipe administrativa, de advogados e em especial aos meus sócios do escritório Leandro Bissoli, Sandra Tomazi, Márcio Chaves, Caroline Teófilo, Marcelo Crespo, que permitiram que eu me dedicasse a este período acadêmico de estudo profundo, para que pudesse nascer uma nova tese para a comunidade jurídica.

Por último, como eu disse, um trabalho desta magnitude não é obra de uma mente apenas, por isso, encerro, fazendo um especial agradecimento a minha família, cujo apoio foi essencial para a realização deste sonho, a minha mãe Jane, minha irmã Danielle, meu irmão Luiz Cláudio, minha sogra Maria da Penha, meu sogro Gabriel, meus filhos Gabriela e Rafael e ao meu esposo, meu grande companheiro e alma gêmea, Romulo Pinheiro, com muito amor, obrigada.

Patricia Peck Garrido Pinheiro.

“Não é a posse da verdade, mas o sucesso que vem após a pesquisa, onde a busca é enriquecida por ela!” (MAX PLANCK (1858-1947))

PINHEIRO, Patricia Peck Garrido. *O direito internacional da propriedade intelectual aplicada à inteligência artificial*. 2018. 316f. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2018.

## RESUMO

O estudo da legislação em vigor, nacional e internacional, sobre a propriedade intelectual das bases de dados é o ponto de partida dessa tese. A investigação apresenta um olhar evolutivo e comparativo do que ocorreu no tratamento da propriedade intelectual das bases de dados desde a Convenção de Berna, do Acordo sobre Aspectos dos Direitos de Propriedade Intelectual Relacionados ao Comércio - TRIPS, da Diretiva Europeia 96/9/EC relativa à Proteção Jurídica das Bases de Dados, da Lei Americana dos Direitos Autorais do Milênio Digital - DMCA e por fim da Lei 9610/98 de atualização de Direitos Autorais no Brasil, com os efeitos recentes das leis sobre proteção de dados pessoais como o Regulamento Europeu (*General Data Protection Regulation* - GDPR) e a lei brasileira (conferida pelo PLC 53 ou Lei Geral de Proteção de Dados Pessoais - LGPD). A pesquisa suscita justamente a verificação da necessidade ou não de se atualizar a proteção jurídica sobre as bases de dados, tendo em vista a transformação tecnológica que ocorre desde os anos 90, período em que a maioria das normas sobre esta matéria foram criadas, até o momento atual, com a aplicação na Inteligência Artificial (IA). Se por um lado, houve um aumento da necessidade das empresas de acessarem e de usarem a informação, seja ela coletada por aplicações da *web*, pelos novos dispositivos de Internet das Coisas (IoT) ou usados no aprendizado de máquina (*machine learning*). Há, ainda, que se levar em consideração questões relacionadas às regras concorrenciais e de livre acesso à informação (direito ao conhecimento), que podem de algum modo limitar os anseios pela proteção deste ativo como uma propriedade intelectual empresarial. Neste contexto, o presente trabalho apresenta um estudo jurídico comparativo para compreender as vertentes seguidas na Europa, nos Estados Unidos e no Brasil com o intuito de atingir uma ampla análise do problema e traçar possíveis caminhos de solução visando um entendimento uniforme. Pensando nessa sociedade digital e na intenção da Organização Mundial do Comércio (OMC) em garantir um fluxo livre de dados entre países (*free data flow*), a tese sugere como uma das respostas às questões atuais sobre a intersecção natural entre o direito internacional da propriedade intelectual e a proteção da privacidade dos dados pessoais quando se trata da sua aplicação na internet e na inteligência artificial, a necessidade de elaborar um tratado multilateral com o intuito de atingir um consenso mínimo de quem teria direitos sobre a propriedade, o acesso e o uso das bases de dados digitais. Busca-se uma melhor resposta para tratar adequadamente este ativo tão valioso que envolve não apenas as bases de dados chamadas de primárias, mas até a análise do quanto esta nova camada robotizada será capaz de criar a partir do *machine learning* e se esta criação seria passível de proteção pela propriedade intelectual. Logo, esse novo contexto digital eleva não apenas a complexidade da discussão sobre a propriedade destas bases de dados, quer seja em seu processo tradicional de formação industrial ou em seu processo digital de composição híbrida que inclui também os dados pessoais, mas também o problema que paira sobre a construção de bases de dados derivadas, de conhecimento aprendido por máquina, e em que medida poderiam também ser objeto de proteção pela propriedade intelectual, não apenas por sua organização mas também pelo fato de que sua criação seria realizada por robôs. No contexto econômico do século XXI, cooperação e integração entre os países se tornaram fenômenos extremamente necessários, por isso, por fim, o trabalho conclui com a propositura de algumas estratégias com base nos princípios do Direito Internacional Privado para atender ao objetivo de dar maior eficácia à solução de conflitos envolvendo a matéria, que tem alcance internacional devido a sua natureza multiterritorial (intrínseca a própria internet). Destes princípios repousariam os mais consagrados como o do tratamento nacional, da independência dos registros, da nação mais favorecida, da proteção mínima (*single undertake*), do esgotamento internacional de direitos (exaustão), da transparência, da cooperação internacional mútua, da patenteabilidade absoluta, da interpretação evolutiva e da licença compulsória. E quanto

às estratégias, a proposta seria a da aplicação de novas minutas de contratos com um padrão de cláusulas pré-definidas, que podem ser determinadas por um modelo de *Soft-Law*, e que possibilitem o uso de mecanismos de mediação e de arbitragem internacional para resolução de controvérsias. Afinal, este é o verdadeiro incentivo para os Estados-Membros integrarem o modelo de constelação das Nações Unidas, encontrar respostas para um futuro livre, sustentável, seguro e pacífico.

**Palavras-chave:** Bases de dados. Propriedade intelectual. Privacidade. Internet das Coisas. Inteligência Artificial. Direito de Acesso aos Dados. Tratado internacional. Contrato. Arbitragem.

PINHEIRO, Patricia Peck Garrido. *International Law over Intellectual Property applied to Artificial Intelligence*. 2018. 316p. Thesis (PhD) – Law School, University of São Paulo, São Paulo, 2018.

### ABSTRACT

The study of the current national and international legislation on the intellectual property of databases is the starting point of this thesis. The research brings an evolutionary and comparative view of what has occurred in the treatment of intellectual property of databases since the Berne Convention, the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), European Directive 96/9/EC on Legal Protection of Databases, the Digital Millennium Copyright Act - DMCA and finally the Brazilian updated Copyright Law no. 9610/98, analysing the effects of the recent laws on protection of personal data such as the General Data Protection Regulation (GDPR) and the Brazilian law (conferred by PLC 53 or General Law of Protection of Personal Data - LGPD) and by proposals for the regulation of artificial intelligence of both the European Union and the United States. The research raises precisely whether or not it would be necessary to update the legal protection of the database, bearing in mind the technological transformation that has taken place since the 1990s, when most norms on this matter were created, until the current moment that enterprises are reaching the applications of Artificial Intelligence (IA). On the one hand, there has been an increase in the need for companies to access and use information, whether collected by web applications or by new devices within the Internet of Things (IoT). Until it reaches the application in machine learning in the AI solutions, making the repositories of information essential for the evolution of the business, on the other hand, there has also been a great increase in regulations regarding the protection of individuals' privacy and personal data, and issues related to competition rules and free access to information (right to know), which may in some way limit the longing for the protection of this asset as an intellectual property business, have to be taken into account. In this context, the dissertation presents a comparative legal study to understand the trends in Europe, the United States and Brazil, to reach a broad analysis of the problem and outline possible solutions based on a uniform understanding. Thinking about this digital society and the intention of the World Trade Organization (WTO) to ensure a free data flow between countries, the thesis suggests as one of the answers to the current questions about the natural intersection between international intellectual property law and the protection of personal data when it comes to its application on the internet and artificial intelligence, the need to develop a multilateral treaty with in order to reach a minimum consensus of those who would have rights over the ownership, access and use of the database, their evolution as machine-learned knowledge database, even the analysis of how much this new robotized layer will be able not only to use these digital databases but also to create and if this creation would be subject to protection by intellectual property. Therefore, this new digital context raises not only the complexity of the discussion about the ownership of these digital databases, whether in its traditional process of industrial formation or in its digital hybrid composition process with the participation of personal databases of Internet users, involving rights of individuals and related third parties, direct or indirectly, to its composition, but also to the problem that arises about the construction of derived databases, of knowledge learned by machine, and to what extent they could also be protected by intellectual property, not only by their organization but also by the fact that its creation would be carried out by robots. Finally, the present work also identifies other strategies based on International Law principles, to meet the objective of giving a better legal effect in conflict settlement regarding this topic, which has an international scope due to its multi-territorial nature (intrinsic to the internet itself). These other strategies are, for example, the application of new draft contracts with a pattern of pre-defined clauses, which can be determined by Soft-Law, and which allows the use of international arbitration and mediation mechanisms for dispute settlements.

**Keywords:** Industrial database. Intellectual property. Privacy. Data access rights. Internet of Things. Artificial Intelligence. International Treaty. Contract. Arbitration.

PINHEIRO, Patricia Peck Garrido. *Geistiges Eigentum versus Privatsphäre von digitalen Datenbanken: Wer sollte Eigentum, Zugang und Nutzung von Rechten an Daten im Zeitalter von Internet of Things (IoT) haben?* 2018. 316s. Thesis (PhD) – Law School, University of São Paulo, São Paulo, 2018.

## ZUSAMMENFASSUNG

Das Studium der aktuellen nationalen und internationalen Gesetzgebung über das geistige Eigentum von Datenbanken ist der Ausgangspunkt dieser Arbeit. Die Forschung bringt eine evolutionäre und vergleichende Sicht auf das, was bei der Behandlung des geistigen Eigentums von Datenbanken seit dem Abschluss unterschiedlicher Vereinbarungen und Gedankenansätze wie die Berner Übereinkunft; das Abkommen über handelsbezogene Aspekte der Rechte des geistigen Eigentums (TRIPS); die europäische Richtlinie 96/9 / EG über Rechtsschutz; der Digital Millennium Copyright Act - DMCA und schließlich dem aktualisierten brasilianischen Urheberrecht Nr. 9610/98, durch Gesetz zum Schutz personenbezogener Daten wie die Allgemeine Datenschutzverordnung (DSGVO); das brasilianische Gesetz (übertragen durch PLC 53 oder Allgemeines Gesetz zum Schutz personenbezogener Daten - LGPD); die Vorschläge zur Regulierung künstlicher Intelligenz sowohl in der Europäischen Union als auch in den Vereinigten Staaten, eingetreten ist. Die Forschung behandelt die Frage, ob es notwendig wäre, den rechtlichen Schutz der Datenbanken zu aktualisieren, unter Berücksichtigung der technologischen Transformation, die seit den 1990er Jahren stattgefunden hat, als die meisten Normen in dieser Angelegenheit erstellt wurden, bis zum gegenwärtigen Moment, mit der Anwendung in Künstlicher Intelligenz (AI). Auf der einen Seite gab es eine Erhöhung der Notwendigkeit für Unternehmen, auf Informationen zuzugreifen und zu nutzen, die entweder von Webanwendungen oder von neuen Geräten im Internet der Dinge (IoT) gesammelt wurden. Auf der anderen Seite hat es auch eine deutliche Erhöhung der Vorschriften über den Schutz der Privatsphäre und der personenbezogenen Daten von Privatpersonen gegeben. Fragen im Zusammenhang mit Wettbewerbsregeln und freiem Zugang zu Informationen (Recht auf Kenntnis), welches das Bedürfnis des Schutzes von geistigem Eigentum einschränken kann, müssen berücksichtigt werden. In diesem Zusammenhang präsentiert die Dissertation eine vergleichende juristische Studie, um die Trends in Europa, den USA und Brasilien zu verstehen, um eine umfassende Analyse des Problems zu erreichen und mögliche Lösungen auf der Grundlage eines einheitlichen Verständnisses darzustellen. Angesichts dieser digitalen Gesellschaft und der Absicht der Welthandelsorganisation (WTO), einen freien Datenfluss zwischen den Ländern zu gewährleisten, befasst sich die vorliegende Arbeit mit der Antworten auf die aktuellen Fragen bezüglich der Schnittstelle zwischen internationalem Recht auf geistiges Eigentum und dem Schutz der Privatsphäre im Umfeld von Internet-Anwendung und künstlicher Intelligenz. Ziel der Studie ist die Entwicklung eines multilateralen Vertrags über einen Mindestkonsens bezüglich der Rechte über Eigentum, Zugang und Nutzung digitaler Datenbanken. Diese Datenbanken werden als Primärdaten bezeichnet: ihre Entwicklung als maschinell erlernte Wissensbasen, die bereits von einem intelligenten Lernalgorithmus und Pseudoanonymisierungsfiltren durchlaufen wurden. Daraus konnten Sekundärdatenbanken erstellt werden. Schließlich wird analysiert, inwieweit diese neue robotisierte Schicht in der Lage sein wird, diese digitalen Datenbanken zu nutzen und zu erstellen, und ob die Erstellung einem Schutz durch geistiges Eigentum unterliegen würde. Dieser neue digitale Kontext erhöht die Komplexität des Problems aufgrund der Einbeziehung des industriellen Prozesses (und des traditionellen Schutzes auf Gerätepatenten) sowie der Rechte von Nutzern und Dritten, die direkt oder indirekt auf Datenbanken, die erstellt oder gesammelt wurden, verknüpft sind. Schließlich identifiziert die Studie auch andere Strategien (basierend auf den Prinzipien des internationalen Privatrechts), um das Ziel zu erreichen, eine bessere Rechtswirkung in der Konfliktlösung zu diesem Thema zu schaffen, das aufgrund seiner multiregionalen Natur (im Internet) selbstverständlich ist. Diese anderen Strategien sind beispielsweise die Anwendung neuer Vertragsentwürfe mit einem Muster von vordefinierten Klauseln, die durch Soft-Law bestimmt werden können und die den Einsatz internationaler Schieds- und Vermittlungsmechanismen für Streitbelegungen ermöglichen.

**Schlüsselwörter:** Industrielle Datenbank. Geistiges Eigentum. Privatsphäre. Datenzugriffsrechte. Internet of Things. Künstlicher Intelligenz (AI). Internationale Verträge. Verträge. Schiedsgericht.

## LISTA DE ILUSTRAÇÕES

Figura 1 – Formação de Bases de Dados Primária ( <i>Data Lake</i> ) .....	65
Figura 2 – Modelo de Negócios da Indústria dos Dados ( <i>Data Industry</i> ) .....	87
Figura 3 - Microsoft. Política de Privacidade .....	129
Figura 4 - Google. Política de Privacidade e Termos de Uso .....	130
Figura 5 - Apple. Política de Privacidade .....	132
Figura 6 - Aviso legal na interface da inteligência artificial com o usuário .....	148
Figura 7 - Estudo de caso da indústria de carro autônomo .....	168
Figura 8 – Modelo de Composição da Inteligência Artificial .....	174
Figura 9 - Matriz de avaliação de ativos de inteligência artificial .....	181
Figura 10 - Matriz de Riscos e Salvaguardas das Bases de Dados de IA .....	204

## LISTA DE QUADROS

Quadro 1 - Análise de Jurisprudência – Caso 1 [2012] C-604/10 – Football Dataco .....	185
Quadro 2 - Análise de Jurisprudência – Caso 2 [2015] C-30/14 – Ryanair Ltd .....	188
Quadro 3 - Análise de Jurisprudência – Caso 3 [2012] 676 F.3d 19 – Viacom Int.....	191
Quadro 4 - Análise de Jurisprudência – Caso 4 [2003] 329 F.3d 9 – Pharmatrak.....	193
Quadro 5 - Análise de Jurisprudência – Caso 5 [1985] QB 526 – Lion Lab.....	194
Quadro 6 - Análise de Jurisprudência – Caso 6 [2017] <i>Preliminary Injunction</i> – Waymo..	195
Quadro 7 - Análise de Jurisprudência – Caso 7 (2012) – Webmotors .....	198
Quadro 8 - Análise de Jurisprudência – Caso 8 (2014) – All Match.....	199
Quadro 9 - Análise de Jurisprudência – Caso 9 (2017) – Jr do Brasil .....	200

## LISTA DE TABELAS

Tabela 1 – Tabela Comparativa dos tipos de dados.....	67
Tabela 2 – Análise comparativa dos direitos intelectuais no Brasil, EUA, UE .....	101
Tabela 3 - Regulamentações sobre Propriedade Intelectual no Brasil e Europa.....	103
Tabela 4 - Tabela comparativa Regulamentação Brasileira e Europeia de Proteção de Dados Pessoais .....	142
Tabela 5 - Análise dos princípios ALI, CLIP e sua aplicação para a Internet .....	145

## LISTA DE SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
ADR	Adequate Dispute Resolution methods
ALI	American Law Institute
BGH	Bundesgerichtshof (Tribunal Federal de Justiça da Alemanha)
CDADC	Código de Direito de Autor e dos Direitos Conexos de Portugal
CEDPI	Centro de Defesa de Propriedade Intelectual
CIDIPs	Convenções Interamericanas de Direito Privado
CIJ	Corte Internacional de Justiça
CLIP	Conflicts of Laws in Intellectual Property
CNJ	Conselho Nacional de Justiça
CPJI	Corte Permanente de Justiça Internacional
CTEA	Sonny Bono Copyright Term Extension Act
CUB	Convenção de Berna
CUP	Convenção de Paris
DBMS	Data Base Management System
DIPr	Direito Internacional Privado
DMCA	Digital Millennium Copyright Act de 1998
DRM	Digital Rights Management
EUA	Estados Unidos da América
GATS	Acordo Geral de Tarifas de Comércio em Serviços
GATT	Acordo Geral de Tarifas de Comércio
GDPR	General Directive Privacy Regulation
GEMA	Instituição Alemã de Gestão Coletiva de Direitos Autorais
IAB	Internet Architecture Board
ICANN	Internet Corporation for Assigned Names and Numbers
IDI	Instituto de Direito Internacional
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
INPI	Instituto Nacional de Propriedade Intelectual
IoT	Internet of Things
IP	Internet Protocol
IRTF	Internet Research Task Force
ISOC	Internet Society
ISP	Internet Service Provider
LAI	Lei de Acesso a Informação
MIT	Massachusetts Institute of Technology

MPG	Max Planck Institute for Innovation and Competition
OEA	Organização dos Estados Americanos
OMC	Organização Mundial do Comércio
OMPI	Organização Mundial de Propriedade Intelectual
ONG	Organização Não Governamental
ONU	Organização das Nações Unidas
PI	Propriedade Intelectual
TCP	Telecomunicação com Pacotes
TFEU	Treaty on the Functioning of the European Union
TIEF	Tratado sobre Interpretação e Execução de Fonogramas
TJUE	Tribunal de Justiça da União Europeia
TRIPS	Acordo sobre os Aspectos dos Direitos de Propriedade Intelectual Relacionados ao Comércio
UDRP	Uniform Dispute Resolution Policy
UE	União Europeia
UNCITRAL	Comissão das Nações Unidas para o Direito Comercial Internacional
UNIDROIT	Instituto Internacional para Unificação do Direito Privado
USP	Universidade de São Paulo
W3C	World Web Consortium
WIPO	World Intellectual Property Organization
WTO	World Trade Organization
WWW	World Wide Web

## SUMÁRIO

<b>INTRODUÇÃO</b> .....	19
1. Apresentação do problema e da contextualização da tese .....	19
2. Objetivos da Pesquisa.....	25
3. Metodologia de Pesquisa .....	27
4. Estrutura do Trabalho.....	28

### PARTE 1

#### A PROPRIEDADE INTELECTUAL DAS BASES DE DADOS NA ERA DIGITAL

#### **CAPÍTULO 1. A PROPRIEDADE INTELECTUAL SOBRE AS BASES DE DADOS NA ERA DIGITAL**..... 33

1.1. A informação como um bem livre da Sociedade do Conhecimento .....	33
1.2. Conceito de bases de dados .....	39
1.3. Os direitos envolvidos nas bases de dados .....	45
1.4. A proteção das bases de dados como um direito <i>sui generis</i> .....	47
1.5. O requisito da originalidade.....	56
1.6. A repressão a concorrência desleal como escopo do direito <i>sui generis</i> .....	57

#### **CAPÍTULO 2. OS DESAFIOS SOBRE A PROTEÇÃO DAS BASES DE DADOS DIGITAIS COM OS NOVOS AVANÇOS TECNOLÓGICOS** .... 61

2.1. A quebra do paradigma do suporte físico e a internet.....	61
2.2. Análise da formação das bases de dados na era digital.....	63
2.2.1. Empresariais .....	65
2.2.2. Pessoais.....	65
2.2.3. Híbridas.....	66
2.2.4. Tabela Comparativa dos tipos de dados .....	66

### PARTE 2

#### A NATUREZA INTERNACIONAL DA SOCIEDADE DIGITAL

#### **CAPÍTULO 3. A NATUREZA INTERNACIONAL DA PROPRIEDADE INTELECTUAL**..... 71

3.1. Sociedade da Informação, mercados digitais e propriedade intelectual .....	71
3.2. A propriedade intelectual no Ordenamento internacional .....	74
3.3. Análise histórica entre os sistemas <i>Urheberrecht</i> , <i>Copyright</i> e <i>Droit D´auteur</i> , e a matriz de um direito de propriedade intelectual comunitário .....	89
3.4. Panorama regulatório: estudo comparativo das legislações aplicáveis no tocante a propriedade intelectual, direitos de uso e acesso às bases de dados .....	99

<b>CAPÍTULO 4. A NATUREZA INTERNACIONAL DA INTERNET</b> .....	105
4.1. Da <i>Lex Mercatoria</i> à <i>Lex Digitalis</i> : um direito mundial para a Internet .....	105
4.2. Princípios de Direito Internacional Privado aplicáveis à internet .....	114
4.3. A propriedade intelectual na Internet e a questão da territorialidade .....	117

### **PARTE 3**

## **A GOVERNANÇA DAS RELAÇÕES DA INTERNET POR MEIO DOS CONTRATOS**

<b>CAPÍTULO 5. OS NOVOS MODELOS DE NEGÓCIOS E OS TIPOS CONTRATUAIS QUE GERAM EFEITOS EXTRATERRITORIAIS</b> .....	125
5.1. O poder dos contratos na era digital .....	125
5.2. Os termos de uso na internet e seus efeitos jurídicos .....	127

### **PARTE 4**

## **O FUTURO DA REGULAMENTAÇÃO DOS DIREITOS DE PROPRIEDADE, USO E ACESSO DAS BASES DE DADOS DIGITAIS**

<b>CAPÍTULO 6. OS DIREITOS HUMANOS VERSUS A PROPRIEDADE INTELLECTUAL NA SOCIEDADE DO CONHECIMENTO</b> .....	135
6.1. A privacidade como um direito limitador à propriedade das bases de dados .....	135
6.2. A regulamentação da proteção dos dados pessoais e seus impactos sobre os direitos de uso e acesso às bases de dados .....	138

<b>CAPÍTULO 7. PROPOSTAS DE SOLUÇÃO ATRAVÉS DE NOVOS MODELOS QUE POSSAM REGULAR OS DIREITOS DE PROPRIEDADE, USO E ACESSO ÀS BASES DE DADOS DIGITAIS</b> .....	145
7.1. Proposta de criação de um modelo de <i>Soft Law</i> com <i>Standard Clauses</i> para Contratos. ....	145
7.2. Proposta de um Tratado Internacional que regule os direitos de propriedade, acesso e uso as bases de dados digitais .....	148
7.3. Proposta de uso de arbitragem para solução de conflitos (Modelo OMC/WIPO) .....	149

### **PARTE 5**

## **A PROPRIEDADE INTELLECTUAL APLICADA À INTERNET DAS COISAS E À INTELIGÊNCIA ARTIFICIAL**

<b>CAPÍTULO 8. OS NOVOS MODELOS DE NEGÓCIOS COM A INTERNET DAS COISAS</b> .....	157
8.1. A Internet das Coisas: conceito e efeitos jurídicos .....	157
8.2. A propriedade das bases de dados na Internet das Coisas .....	162
8.3. Estudo de caso prático .....	167
8.3.1. Indústria de automóveis .....	167

<b>CAPÍTULO 9. A EVOLUÇÃO PARA A INTELIGÊNCIA ARTIFICIAL</b> .....	171
9.1. O novo paradigma ético e jurídico da Inteligência Artificial .....	171
9.2. A propriedade intelectual na Inteligência Artificial.....	172
9.3. O direito internacional aplicado à Inteligência Artificial e as tendências regulatórias da União Europeia e dos Estados Unidos .....	176
9.4. Análise jurisprudencial comparada sobre casos envolvendo bases de dados.....	182
<b>CONCLUSÃO</b> .....	203
<b>REFERÊNCIAS</b> .....	219
<b>ANEXOS</b> .....	231
ANEXO A: Análise Jurisprudencial Sobre Casos Envolvendo Bases de Dados (Brasil) .....	233
ANEXO B: Análise Jurisprudencial Sobre Casos Envolvendo Bases de Dados (Europa).....	251
ANEXO C: Análise Jurisprudencial Sobre Casos Envolvendo Bases de Dados (EUA).....	273
ANEXO D: Pesquisa Internacional .....	313



# INTRODUÇÃO

## 1. Apresentação do problema e da contextualização da tese

Hoje, as pessoas que detêm ideias são mais poderosas do que aquelas que operam máquinas e, em muitos casos, até mais do que aquelas que possuem essas máquinas. O mundo está mudando em direção a uma economia que depende mais da criatividade e do conhecimento do que de qualquer outra matéria prima, incluindo o petróleo.<sup>1</sup>

“Não é o mais forte que sobrevive, nem o mais inteligente, mas o que melhor se adapta às mudanças” (CHARLES DARWIN - 1809 a 1882).<sup>2</sup>

“Em tempos de renovação dos métodos e da globalização do ensino jurídico, deve o jurista internacional buscar inspiração na totalidade do direito, sem perder de vista a variedade de suas áreas especializadas”<sup>3</sup>

Inicialmente, pode-se afirmar que a internet trouxe, de certa maneira, uma dimensão de vida mais internacional, porém pela via digital, para todos os indivíduos que estão conectados na rede, mesmo que eles nunca deixem fisicamente os seus países de origem ou sequer tirem um passaporte.

Adentramos os anos 2000 com a propriedade intelectual sendo a grande plataforma econômica da sociedade digital. Segundo Manuel Castells: “as novas tecnologias da informação não são simplesmente ferramentas a serem aplicadas, mas processos a serem desenvolvidos. Pela primeira vez na história, a mente humana é uma força direta de produção, não apenas um elemento decisivo no sistema produtivo”.<sup>4</sup>

De certo modo, desde a Convenção de Berna (“*First Multilateral International Copyright Treaty*”), a proteção dos direitos intelectuais tem ido ao sabor dos interesses de desenvolvimento econômico dos países. O sistema atual vigente foi feito para evitar conflitos. A função do Acordo sobre os Aspectos dos Direitos de Propriedade Intelectual

---

<sup>1</sup>HOWKINS, John. *The creative economy*. São Paulo: Ed. Mbooks, 2012. p. 16. O jornalista John Howkins é autor da obra *Economia Criativa* (Editora MBooks, 2012).

<sup>2</sup>Frase atribuída a Charles Robert Darwin, proferida em 1963 por Leon C. Megginson, professor da Louisiana State University, num discurso sobre sua interpretação da obra “On the origins of species by means of natural selection – on the preservation of favoured races in the truggle for life” de Charles Robert Darwin.

<sup>3</sup>BASSO, Maristela. *Curso de direito internacional privado*. 3. ed. São Paulo: Atlas, 2013. p. 49.

<sup>4</sup>CASTELLS, Manuel. *A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade*. Tradução de Maria X. De A. Borges. Rio de Janeiro: Jorge Zahar, 2013.

Relacionados ao Comércio (TRIPS) foi a de robustecer o sistema anterior que era a Organização Mundial de Propriedade Intelectual (OMPI), manter sua complementariedade e sua interpretação evolutiva.

Há uma fraternidade entre o livre comércio e a proteção dos direitos intelectuais. No entanto, quando há conflito, é de interpretação e, normalmente, é na aplicação da lei interna. Por isso, deve ser aplicado o princípio da interpretação consistente como compromisso com o plano internacional. Para José de Oliveira Ascensão<sup>5</sup>, a sociedade da informação teve um elevado peso na globalização dos direitos intelectuais.

Mas, devido ao fato de a propriedade intelectual ser considerada como um direito humano<sup>6</sup>, como tal, sendo um bem, um ativo, também acabou por tornar-se objeto de comércio. E isso, por si só, trouxe elementos de polêmica e de perturbação para este instituto desde a sua concepção. Restando, ainda, mais agravado com o aumento da relevância das bases de dados para a Sociedade, que está cada vez mais dependente de informação. Daí o grande paradigma: garantir um direito de exclusividade (propriedade) sobre os dados (e bases de dados) ou garantir o livre acesso a informação.

A temática das bases de dados, de certo modo, chamou a atenção do mundo nos anos 90, mas depois foi abandonada pela comunidade internacional. Por quê? A tese inicia justamente em busca desta resposta e promove uma vasta análise das diferenças e das semelhanças, justapondo o que já é conhecido com as recentes descobertas técnicas e suas aplicações cujos impactos ainda são desconhecidos pela comunidade jurídica, com observância não apenas de fatores legais, mas dos comportamentos atuais do mundo globalizado e conectado pela internet, em uma forma não imaginada na época dos anos 90, que fará surtir a revelação necessária da importância de se retomar a discussão desta matéria.

---

<sup>5</sup>ASCENSÃO, José de Oliveira. Sociedade da informação e mundo globalizado. In: WACHOWICZ, Marcos (Coord.). *Propriedade Intelectual & Internet*. 1. ed. (ano 2002), 4. tir. Curitiba: Juruá, 2005. p. 15-31.

<sup>6</sup>Conforme celebrado no artigo 27.2 da Declaração Universal dos Direitos do Homem: “*todo homem tem o direito à proteção dos interesses morais e materiais decorrentes de qualquer produção científica, literária ou artística da qual seja autor*” e no Pacto Internacional sobre Direitos Econômicos, Sociais e Culturais, artigo 15.c: “1. O direito de toda pessoa de beneficiar-se da proteção dos interesses morais e materiais que os correspondam por razão das produções científicas, literárias ou artísticas de que seja autora é um direito humano, que deriva da dignidade e dos valores inerentes a toda pessoa. 2. Em contraste com outros direitos humanos, os direitos de propriedade intelectual são geralmente de índole temporal e é possível autorizar seu exercício ou cedê-los a terceiros. (...) 4. O direito de toda pessoa de beneficiar-se da proteção dos interesses morais e materiais que os correspondam por razões de produções científicas, literárias ou artísticas de que seja autora tem por finalidade fomentar a contribuição ativa dos criadores às artes, ciências e ao progresso da sociedade em seu conjunto”.

Quem cria os novos desafios que o direito deve enfrentar é a sociedade, é o princípio da autonomia social. A sociedade cria comportamentos vinculantes. Atualmente, se um usuário de internet quiser usar um aplicativo de comunicação terá que aceitar as regras de uso do serviço e a sua política de privacidade. Está sob a égide da liberdade dos contratos. O mesmo ocorre com o serviço de aplicativo de táxi.

Mas, e quando chegarmos no uso massificado da Internet das Coisas no dia-a-dia dos indivíduos, será que podemos estar sob os mesmos códigos de conduta e de regras contratuais atuais? Ou será necessário celebrar pelo menos uma norma de princípios para reger algumas premissas, em nível internacional, e garantir um padrão mínimo de conduta aceitável nestes ambientes, especialmente em um contexto de cidades, casas, carros, geladeiras, afinal, tudo inteligente, conectado, gerando e coletando dados?

A quem caberia a propriedade destes dados? E das bases de dados? A quem cabe os direitos de uso? E de acesso? Como protegê-las sem retirar a liberdade da informação? E como ficam as responsabilidades? Quem são as partes envolvidas, quem são os terceiros? Quem será imputável? Como avaliar o patrimônio de uma empresa que passa a fabricar dispositivos de *Internet of Things* (IoT) e deter todo este valor de bases de dados (é uma riqueza, por ser um bem, ou é um risco, por ser um ônus)?

Além disso, a tese buscou investigar melhor a presença do fenômeno de ocidentalização do oriente seguido da ocorrência de “transplantes legais”, especialmente no tocante a leis europeias, com a crença na utilidade e na necessidade. Está havendo um predomínio das regras das Diretivas Europeias para dar os ditames sobre diversas matérias para o restante dos demais países, em um processo inclusive de “substantivação” das normas de conflitos, que passam a assumir características temáticas deduzidas a partir de uma coletânea de casos mistos jusprivatistas internacionais.

Deste modo, devido a esta complexidade, verificou-se na pesquisa preliminar que o Direito Internacional Privado (DIPr) seria a disciplina mais adequada para recepcionar a discussão sobre as relações jurídicas em torno da disputa sobre os direitos das bases de dados, por ser mais contemporâneo com os elementos conflituais estrangeiros e os fenômenos dos novos tempos frente os impactos da globalização e das tecnologias digitais que relativizaram sobremaneira as fronteiras entre os países e as suas soberanias nacionais em termos de controle de circulação de bens imateriais pelas vias eletrônicas.

Segundo ensinamento de Maristela Basso:

DIPr oferece soluções que buscam racionalizar esses conflitos, especialmente por meio de critérios de continuidade (evitar a fragmentação do direito, já que este se interpreta e aplica em sua unidade) e a normalização das relações jurídicas (no sentido de fazer aplicar as normas jurídicas pertinentes – ‘normas’ sob uma perspectiva mais ampla.<sup>7</sup>

O motivo da escolha da comparação dos 3 (três) ordenamentos jurídicos, quais sejam o Brasileiro, o Europeu e o Norte-Americano foi devido a intenção de se buscar uma linguagem jurídica mais neutra, com termos e conceitos diferentes dos da linguagem jurídica nacionais, se tomado apenas isoladamente, visando alcançar um entendimento mais harmônico sobre a matéria que possa ser aplicado como medida de solução e resposta para os problemas já enfrentados pela sociedade no tocante a dimensão mais sensível das pessoas: seus dados.

Além disso, também foi observada a possibilidade de se verificar a existência de uma embrionária Ordem Pública Digital, supranacional que permitisse apresentar soluções uniformes e harmonizadas, até mesmo uma suposta *lex mercatória eletrônica (ou digital)* visto o grande pluralismo dos ordenamentos jurídicos envolvidos pela Sociedade em rede.

Sendo assim, uma das reflexões que se buscou chegar sobre o tema foi: será que bases de dados por sua essencialidade relacionada à liberdade de informação, estariam mais para o direito essencial ao oxigênio ou o direito à água?

Destaque-se, por oportuno, que o Direito Internacional, tem suma importância como mecanismo conciliador de vários aspectos da vida internacional das pessoas e que, desde o século XX<sup>8</sup>, Estados europeus e latino-americanos concluíram importantes tratados sobre conflitos de leis em matérias de nacionalidade, domicílio de pessoas, prestação de alimentos, proteção da criança, até mesmo sobre usos das águas e do desenvolvimento sustentável, na busca do equilíbrio no uso equitativo e racional dos recursos hídricos devido ao fato de ser um direito humano universal o acesso à água. Isso fez surgir, inclusive, o Comitê Internacional pelo Contrato Mundial da Água.

A água é um dos grandes temas de discussão entre os Estados, especialmente os que compartilham recursos nas mesmas bacias hidrográficas. Para o Direito Internacional, a

---

<sup>7</sup>BASSO, Maristela. op. cit., p. 22.

<sup>8</sup>Vide Convenção de Haia sobre Nacionalidade de 12 de abril de 1930, Tratado de Direito Internacional Privado de 20 de fevereiro de 1928 (“Código de Bustamante”).

questão da água é analisada tanto como fonte de conflitos quanto como fonte de investimentos entre os respectivos Estados Nacionais. E podemos dizer que os dados estão para a Economia digital do século XXI como a água estava para a economia da sociedade do século XX.

Segundo a visão de Jane Ginsburg<sup>9</sup>, “a propriedade intelectual é, por sua própria natureza, de dimensão internacional”. Pode-se afirmar que a propriedade intelectual é o campo dos direitos individuais mais internacionalizado, vide o colchão único de harmonização promovido pela OMPI e pelo TRIPS. Mas o que mais interessa na experiência comparada é ver como a magistratura interpreta a lei. Daí ter-se dado especial atenção para a análise das decisões judiciais mais recentes sobre a matéria das bases de dados.

Mas não se pode negar que a informação tenha virado moeda de troca e que muitos serviços gratuitos possuem justamente este modelo da gratuidade permutada por dados de seus usuários, de maneira que então estas bases de conhecimento devam ser protegidas como patrimônio destas empresas.

Portanto, esta é a nova fronteira de discussão da propriedade intelectual e que dependerá muito do uso dos princípios e das ferramentas do direito internacional, pois não será com leis nacionais e locais que se poderá enfrentar e resolver adequadamente esta questão.

Mas, claramente, há uma dupla faceta da propriedade intelectual que deve ser observada para que se possa estabelecer um ambiente de desenvolvimento sustentável: por um lado há o interesse privado, o que se bem definido pode deliberar um fluxo vantajoso para pujança econômica de um país. De outro lado, há o interesse público a nortear a necessidade de se garantir o acesso à informação, ao conhecimento, à tecnologia.

Na maioria das vezes, um determinado recurso privado ou natural pode estar em uso pela sociedade por muito tempo sem necessidade de ser objeto de regulamentação internacional, mas ganha esta relevância ao longo do tempo. Segundo Hobsbawm<sup>10</sup>, foi a partir do séc. XVIII, mais especificamente na Inglaterra, que a utilização da água ganhou

---

<sup>9</sup>Jane Ginsburg é professora e leciona Propriedade Intelectual na Faculdade de Direito da Universidade de Columbia nos EUA; também é Presidente da filial norte-americana da Associação Litterarire et Artistique Internationale (ALAI), fundada em Paris em 1878 pelo próprio Victor Hugo. É autora da obra *International Copyright and Neighboring Rights: The Berne Convention and Beyond*, Oxford University Press, 2006. RICKETSON, Sam; GINSBURG, Jane. *International copyright and neighboring rights: the Berne Convention and Beyond*. Oxford University Press, 2006. p. 25.

<sup>10</sup>HOBBSAWM, Eric J. *Da Revolução Industrial inglesa ao Imperialismo*. Rio de Janeiro: Forense-Universitária, 1983. p. 106.

força devido a dois fatores: crescimento da população e o aumento da industrialização da produção. O que promoveu uma profunda mudança social, econômica, política, cultural, tecnológica de 1789 a 1848, período das revoluções na Europa (entre a Revolução Francesa e a Industrial).

Ou seja, a tese buscou investigar os fatos mais recentes sobre as bases de dados em seu fenômeno social e econômico, fora do Direito, para poder redesenhar o melhor modelo jurídico para o seu tratamento, que pode não ter mais nada a ver com o que foi pensando pelas legislações que estão em vigor atualmente, tanto em nível nacional quanto internacional.

Assim, como o tema da água está dentro do rol de direitos essenciais, conforme afirma René Cassin, principal relator da Declaração Universal dos Direitos Humanos, também está o tema da propriedade intelectual, e, dentro dele, o das bases de dados.

Por isso, no que tange ao tema de bens intelectuais, de estímulo à inovação, há a necessidade permanente de renovação e atualização de marcos legais, para que seja possível a manutenção da equação “*checks and balances*” no mercado, pois ele, por sua própria natureza, tende ao desequilíbrio, devido aos diversos interesses envolvidos.

Efetivamente, existe uma grande necessidade de se produzir soluções jurídicas, para o presente e para o futuro. Diante disso, dentro da tese, passou-se a se investigar outras fontes do Direito Internacional Privado (DIPr) que podem contribuir para construção deste futuro, em especial as técnicas de inspiração ou persuasão chamadas de *Soft Law*.

Por último, conforme as lições de Norberto Bobbio<sup>11</sup>, após o declínio do isolamento nacional, há uma tendência do Direito Internacional em se preocupar com o futuro da humanidade. E o Direito Comparado por certo desempenha um papel fundamental para fomentar o comércio internacional, melhorar a qualidade de vida, por intermédio do processo de macrocomparação e microcomparação, consegue estabelecer princípios gerais do Direito reconhecidos pelas nações civilizadas, servindo como um denominador comum, uma ponte cultural-política e jurídica entre elas.

A dimensão social da Revolução digital que se vive parece destinada a cumprir a primeira lei de Melvin Kranzberg:

---

<sup>11</sup>BOBBIO, Norberto. *A era dos direitos*. Tradução de Carlos Nelson Coutinho. Rio de Janeiro: Campus, 2010.

A tecnologia não é boa, nem má e também não é neutra. Com isso pretendo dizer que a interação da tecnologia com a ecologia social é tal que os desenvolvimentos técnicos frequentemente têm consequências ambientais, sociais e humanas que vão muito além dos próprios objetivos imediatos dos dispositivos técnicos e das práticas em si, e a mesma tecnologia pode ter resultados muito diferentes quando introduzida em contextos diferentes ou sob diferentes circunstâncias.<sup>12</sup>

Concluindo, o Direito Internacional Privado juntamente com o Direito Comparado, por seu poder funcional, são a melhor solução para realizar o Direito em uma Sociedade Digital que não conhece fronteiras territoriais para os fluxos de dados digitais.

## 2. Objetivos da Pesquisa

O objetivo da presente tese é realizar uma profunda comparação sobre os direitos relacionados à propriedade intelectual das bases de dados, relacionando semelhanças e diferenças no tratamento em três principais sistemas jurídicos vigentes.

É inquestionável que, na efetivação da proteção da propriedade intelectual no meio digital, a tecnologia acaba por ditar o que é possível de ser feito. A revolução digital mudou a forma de se gerenciar os meios de reprodução, distribuição e publicação da propriedade intelectual.<sup>13</sup>

Se para a propriedade intelectual não seria possível a proteção da ideia pura, abstrata, não exteriorizada em algum tipo de suporte, visto que isso iria contrariar os preceitos da liberdade de criação e da livre iniciativa, da livre circulação do próprio comércio internacional, o que dizer sobre o tráfego de dados, de informações na internet? Seria possível se apropriar destas bases de conteúdos produzidas aos milhares todos os dias e extraí-las do domínio público-coletivo?

Na Agenda 2030 para o Desenvolvimento Sustentável da Organização das Nações Unidas (ONU), os Estados-membros reconheceram a importância da expansão das tecnologias da informação, das comunicações e da interconexão mundial, destacando a necessidade de enfrentar as profundas desigualdades digitais e desenvolver as sociedades do conhecimento, com base em uma educação inclusiva, equitativa, não discriminatória e com

---

<sup>12</sup>KRANZBERG, Melvin. Technology and history: "Kranzberg's Laws". *Technology and Culture*, v. 27, n. 3, p. 545-546, 1986.

<sup>13</sup>BARLOW, John P. The economy of ideas. *Wired online*, 2 Mar. 1994. Disponível em: <<http://homes.eff.org/~barlow/EconomyOfIdeas.html>>. Acesso em: 13 jul. 2017.

respeito às diversidades culturais. Ou seja, há uma grande preocupação da comunidade internacional sobre o destino do uso da informação que é capturada da internet.

O que significa que haverá uma tendência de se gerar mecanismos de controle tecnológico para garantir eficácia jurídica para a proteção dos bens imateriais e isso provavelmente será retratado em futuros tratados ou convenções internacionais sobre a matéria, especialmente no tocante aos direitos autorais.

Para melhor demarcar o problema, o principal objeto que incidirá a comparação será sobre a natureza da proteção jurídica das bases de dados. Portanto, mister se faz conceituar de forma bem clara e objetiva o que são bases de dados, tendo em vista as regulamentações em vigor, que definiram as regras jurídicas a respeito do assunto, mas refletindo um cenário tecnológico anterior ao atual, notadamente a partir dos anos 90.

Em seguida, propõe-se executar uma evolução interpretativa do conceito para os dias de hoje, de modo a adaptar para os desafios que já são enfrentados pelas empresas, buscando transportar para uma solução que possa atender as tendências futuras que este instituto ainda passará em termos de transformações e que já podem ser evidenciadas a partir das análises de casos que serão apresentadas em um capítulo próprio.

Diante disso, buscou-se alcançar uma comparação mais aprofundada dos dois sistemas atuais que possuem visões completamente antagônicas sobre a matéria das bases de dados: o sistema europeu e o sistema norte-americano. E, a partir daí, analisar estes impactos frente à legislação em vigor no Brasil e a tendência de reforma da lei brasileira de direitos autorais para se vislumbrar que caminhos deveriam ser adotados pelo jurista nacional, de modo a ficar melhor equacionada a questão diante de um cenário de entendimentos internacionais contrapostos e até mesmo divergentes sobre o tema.

Ademais, também pretendeu-se desenvolver uma melhor metodologia para interpretação e aplicação das regras de direito internacional privado sobre a matéria na análise dos casos concretos, apresentados em capítulo próprio, visto que tendem a aumentar envolvendo a matéria, para permitir integrar melhor o conhecimento e assim suprir as lacunas que hoje afligem os julgadores nos diversos países, visto que o tema é multiterritorial, transnacional e transcultural.

Por último, tem-se a pretensão de que a presente tese possa servir como instrumento de política legislativa para inspirar possíveis regulamentações sobre o tema, quer seja no formato de *Soft Law* ou *Hard Law*.

O objetivo final é trazer o senso de utilidade para o presente trabalho, no sentido de benefício como ferramenta de construção e de reforma para aplicação, inclusive, em países em desenvolvimento, de modo a reduzir e eliminar discrepâncias, permitindo, assim, facilitar negócios internacionais na medida em que lança luz sobre o desconhecido, o que permite diminuir o medo e a insegurança jurídica nas relações entre diferentes povos e Estados.

### **3. Metodologia de Pesquisa**

O presente trabalho foi desenvolvido, principalmente, com base no método comparativo-dedutivo. Para que pudesse ser promovida a comparação, primeiramente, buscou-se realizar uma análise detalhada do tema no tocante às normas jurídicas envolvidas, os costumes, as ideias, as jurisprudências, bem como os instrumentos de interpretação que estão sendo utilizados atualmente para compreensão de todos os efeitos sociais e econômicos da mudança de comportamento da Sociedade com os novos fluxos de dados digitais.

Assim, visando maior objetividade e resultado, a comparação ficou restrita às ordens jurídicas que estão em contato com a situação controvertida, qual seja, a discussão sobre de quem é o direito de propriedade, do uso e do acesso das bases de dados, com ênfase àquelas que são geradas em suportes eletrônicos (digitais), especialmente oriundas de aplicações da *web* e de dispositivos que já possuem internet das coisas, em um cenário crescente de maior proteção da privacidade dos usuários. E como deve-se buscar àqueles com maior influência sobre a construção do instituto jurídico em questão, há hoje uma bipolaridade de visões, entre a Europa e os EUA.

Frise-se, por oportuno, que a experiência da Comunidade europeia demonstrou-se muito enriquecedora para o presente estudo visto que já retrata uma prática comunitária, onde o legislador buscou alinhar o direito interno com as regras supranacionais.

Portanto, a proposta foi a de que a comparação fosse realizada a partir destes dois sistemas com visões praticamente opostas (europeu e norte-americano) e, a partir deles, trazer para uma análise comparada com o Brasil, para então sugerir uma proposta de solução que possa atender às necessidades brasileiras de atualização da sua própria legislação, como servir de diretriz para se desenvolver um caminho para uma harmonização internacional sobre a matéria.

Desse modo, vislumbrou-se uma comparação em dois níveis: o primeiro nível, de macrocomparação, que consiste na conferência dos sistemas jurídicos envolvidos para classificar e comparar a família de direitos (sua origem), visto que isso afetará a conclusão.

E, em seguida, será aplicado o método da microcomparação, onde se buscará comparar os institutos jurídicos afins dos ordenamentos jurídicos distintos com relação a sua possível inclusão, exclusão ou interseção sobre o objeto de estudo comparativo.

Destaque-se que foi aplicado o método de comparação funcional, ou seja, foram usados questionários para apurar o entendimento sobre o assunto junto aos especialistas nas diversas localidades (*factual approach*), com uso de pesquisa empírica.

Isso se deveu ao fato do ineditismo da temática abordada e a escassez de referências mais recentes, visto que muitas obras publicadas retratam o espírito jurídico dos anos 90 e início dos anos 2000, para o melhor progresso do desenho de uma metodologia própria de microcomparação baseado no método fático-funcional com questionário com formação de grupos de entrevistados de juristas de diversos países.

Por isso, o conhecimento do contexto histórico também é fundamental como ferramenta para aplicação do Direito Comparado, devido a seus fatores típicos e atípicos. É por este motivo que o uso da técnica comparativa traz completa aderência ao resultado que se quer alcançar, visto que o Direito Comparado consiste em um processo para se detectar o invisível que se esconde sobre o visível, conforme será demonstrado no tocante a propriedade intelectual das bases de dados.

Como a lei interna (nacional) é considerada pela doutrina como uma das principais fontes normativas do DIPr, é essencial a análise das regulamentações dos 3 ordenamentos jurídicos envolvidos na comparação no que diz respeito à propriedade intelectual das bases de dados e também às regras que, de algum modo, podem afetar os direitos daqueles que sejam seus fabricantes ou titulares (como as leis relacionadas à concorrência, ao consumidor, à privacidade e à proteção de dados).

Como resultado, buscou-se alcançar um melhor conhecimento do sistema jurídico e de seus institutos, contribuindo para o direito nacional, bem como para o direito privado internacional, propiciado pela evidência de originalidade do tema em análise e sua atualidade.

#### **4. Estrutura do Trabalho**

Tendo em vista a contemporaneidade do tema e a complexidade da análise comparativa enfrentada envolvendo a análise do sistema europeu, o sistema norte-americano e o sistema brasileiro no que se refere ao direito internacional da propriedade intelectual sobre as bases de dados em um contexto de internet das coisas (IoT) e inteligência artificial

(IA), a tese está estruturada em 5 partes, 9 capítulos e a conclusão para facilitar a melhor compreensão do assunto.

A primeira parte buscou tratar da justificativa do estudo da propriedade intelectual das bases de dados na era da internet e o porquê da sua importância e urgência para a comunidade jurídica internacional. Além da parte introdutória, ela reúne toda a explanação conceitual sobre o que são as bases de dados, trazendo a evolução histórica do instituto bem como detalha o que há de leis aplicáveis a matéria tanto em nível internacional como nacional, considerando os países objetos de comparação.

Também são tratados, nesta primeira parte, os desafios sobre a proteção das bases de dados diante dos novos avanços tecnológicos, com a análise dos principais impactos da quebra do paradigma do suporte físico para a proteção da propriedade intelectual e as transformações causadas com o advento da internet. Nesta parte também é apresentada uma fórmula de classificação dos tipos de bases de dados formadas a partir dos meios digitais que se propõe a facilitar o enquadramento jurídico aplicável para a proteção que se quer imprimir as mesmas.

Na segunda parte foi abordada a natureza internacional da propriedade intelectual e da própria sociedade digital conectada através da internet, com análise histórica e comparada entre os sistemas *Urheberrecht*, *Copyright* e *Droit D'auteur*, para apresentação da matriz do direito de propriedade intelectual comunitário vigente atualmente, seus principais pontos de semelhança e diferença.

Também buscou-se investigar mais a fundo sobre a possibilidade da existência de uma Ordem Pública Digital e a formação do que poderia ser chamado de uma *lex mercatoria eletrônica ou digital*. Com isso foram apresentados os princípios fundamentais do Direito Internacional Privado aplicáveis à proteção da propriedade intelectual na internet e analisada a questão da territorialidade e do conflito das leis no espaço. Ao final, buscou-se demonstrar um panorama regulatório geral, comparativo, entre os três sistemas pesquisados: o brasileiro, o europeu e o norte-americano, através de uma análise com 10 indicadores.

A terceira parte do trabalho consiste na observância da aplicação dos contratos como medida jurídica mais imediata para a governança das relações de indivíduos e instituições através da internet, bem como para dar tratamento às lacunas relacionadas às questões da propriedade das bases de dados em plataformas digitais. Para tanto, foi feito um mapeamento do que tem sido aplicado pelas principais empresas que representam a economia digital e

detêm grande parcela da captura dos dados e cujo valor das ações (patrimônio empresarial) está diretamente relacionado ao valor econômico dos seus bancos de dados.

Portanto, qualquer risco na proteção jurídica dos mesmos traz um impacto direto para estas empresas e para os ecossistemas mercadológicos nos quais estão inseridas. Ademais, dentro desta parte, dedicou-se especial atenção – em capítulo próprio – às novas relações trazidas com o uso da internet das coisas e na apresentação de casos práticos de algumas indústrias relevantes e jurisprudências recentes sobre discussões no tocante a propriedade de bases de dados.

Na quarta parte da tese o olhar passou a ser sobre o futuro das regulamentações dos direitos intelectuais sobre as bases de dados e o paradigma entre a propriedade intelectual e os direitos humanos, especialmente a liberdade de informação e a privacidade, considerando o novo arcabouço jurídico de regulamentações sobre proteção de bases de dados pessoais tais como o Regulamento Geral Europeu (GDPR) e a tramitação da lei brasileira (LGPD) e usa intersecção na medida em que se constituam elementos limitativos à garantia da proteção propriedade das bases de dados.

Na última parte buscou-se responder ao problema apresentado concluindo com uma síntese histórica, evolutiva e comparada, já considerando um cenário sócio-econômico de avanços tecnológicos no uso de IoT e IA. Sendo assim, dedicou-se este último capítulo para apresentar estudos de casos de jurisprudência comparada dos sistemas Europeu, Norte-Americano e Brasileiro e por último buscou-se apresentar algumas propostas de solução através de modelos novos que possam regular melhor a questão das bases de dados a partir de tudo que foi analisado, fechando com as conclusões.

## CONCLUSÃO

O objetivo do presente trabalho foi o de investigar as possíveis respostas para o problema relacionado à necessidade de se garantir um regime de proteção das bases de dados na inteligência artificial considerando os institutos e princípios aplicáveis do Direito Internacional Privado e da Propriedade Intelectual bem como identificar novas abordagens e espaços para criação de possíveis novos institutos jurídicos que possam melhor atender a complexidade sócio-econômica dos modelos de negócios atuais e os anseios de ordem pública e privada visando, ao final, o estímulo à inovação mas em conformidade com valores que atendam à proteção da dignidade humana e à livre circulação dos dados (*free data flow*).

Desse modo, buscou-se propor alguns caminhos de solução para criação de um quadro jurídico que pudesse estar melhor adaptado à atual economia dos dados através da eliminação dos obstáculos remanescentes em matéria de circulação de dados e da resolução de incertezas jurídicas criadas pelas novas tecnologias de dados.

Será que se conseguirá alcançar o objetivo do direito internacional privado, de promover uma internacionalização de valores, de forma a harmonizar garantias para toda a comunidade globalizada da “sociedade digital” que está conectada em uma única grande rede chamada “internet” com o fluxo livre de dados entre os países?

Uma boa forma de resumir tudo o exposto é com um dos ensinamentos do José de Oliveira Ascensão<sup>278</sup>: “[...] quem domina a informação domina o mundo.” É o que a Sociedade da informação é, uma grande batalha pela propriedade, pelo acesso, pelo uso, pelo controle dos dados. E quem detiver isso, terá o poder.

Conforme toda a pesquisa realizada para a estruturação do presente trabalho, a temática das bases de dados permite, por sua riqueza e abrangência, a aplicação de todas as fontes do DIPr como um todo, inclusive as elencadas pelo rol do art. 38 do Estatuto da Corte Internacional de Justiça<sup>279</sup>.

---

<sup>278</sup>ASCENSÃO, José de Oliveira. Sociedade da informação e mundo globalizado, cit., p. 19.

<sup>279</sup>Estatuto da Corte Internacional de Justiça, artigo 38: “a Corte, cuja função é decidir de acordo com o direito internacional as controvérsias que lhe forem submetidas, aplicará: a. as convenções internacionais, quer gerais, quer especiais, que estabeleçam regras expressamente reconhecidas pelos Estados litigantes; b. o costume internacional, como prova de uma prática geral aceita como sendo o direito; c. os princípios gerais de direito, reconhecidos pelas nações civilizadas; d. sob ressalva da disposição do Artigo 59, as decisões judiciais e a doutrina dos juristas mais qualificados das diferentes nações, como meio auxiliar para a

Considerando a análise histórica realizada, comparativa e evolutiva dos institutos jurídicos de Direito Internacional Privado e de Direitos Intelectuais, merece dar destaque o fato de que os ativos envolvidos em um contexto de inteligência artificial consistem em: i) Marca; ii) Algoritmo (software); iii) Base de dados primária (não dotada de criatividade mas com elementos únicos de organização e estrutura); iv) Metodologia de aprendizagem de máquina; v) interface/design (ilustração ou desenho industrial); vi) Know-how e segredo de negócios; vii) Base de dados secundária (dotada de elementos de criatividade atribuídos pelo aprendizado de máquina devido a aplicação de *analytics*).

Há portanto, diversos elementos que já são, isoladamente, passíveis de proteção pelo instituto dos direitos intelectuais, demonstrando que então seria mais apropriado que a tutela continuasse a ser tratada pela propriedade intelectual com uma formatação híbrida composta por elementos patenteáveis e outros elementos mais afetos a proteção por direitos autorais.

Segue na Figura 10, um quadro resumo de todos os direitos envolvidos na proteção jurídica das bases de dados, para que se possa compreender sua complexidade e magnitude:

**Figura 10 – Matriz de Riscos e Salvaguardas das Bases de Dados de IA**



Fonte: Próprio autor.

determinação das regras de direito. A presente disposição não prejudicará a faculdade da Corte de decidir uma questão *ex aequo et bono*, se as partes com isto concordarem”.

Émile Durkheim (1893, 1895), um dos fundadores da sociologia, que cunhou o termo “consciência coletiva”, afirmava que o indivíduo é fruto das pressões da sociedade, e é por esse motivo que muitas das suas maneiras de agir com os demais, são de origem coletiva e não somente individual.

No campo dos direitos intelectuais, como assevera Landes e Posner<sup>280</sup>, o princípio básico da propriedade intelectual é o da especialidade da proteção, visto que não é possível se apropriar daquilo que já está em domínio comum. E com isso, se confere um direito de exclusividade para aquele que detém os direitos intelectuais, gerando portanto limitações ou direitos excludentes para os demais.

Ademais, recai o princípio da correção, ou seja, a proteção da propriedade intelectual nunca deverá ser impeditiva para que alguém possa participar e competir em um determinado mercado, mas as condições de sua entrada é que devem ser pautadas em um conjunto de regras para que seja de forma correta. Há, então, todo um sistema concebido com o objetivo de se alcançar um determinado equilíbrio social, cultural e econômico.

E esta fórmula deve ser aplicada com coerência e consistência. Por isso, de modo algum poderia a Sociedade buscar dar o salto do progresso às custas da propriedade privada. Seria o mesmo que dizer que para promover o bem estar social dever-se-ia retirar a legítima propriedade privada da terra. A história tem demonstrado justamente que o progresso deve andar de mãos dadas com a segurança jurídica das relações sociais e empresariais. É bem difícil conceber a liberdade criativa e a sua comunhão com a iniciativa privada sem o sustentáculo da segurança garantida pelas Instituições e pelo Estado.

O aprendizado que cada ente robotizado deve alcançar, seja de modo isolado ou em rede (conectado com seus pares) deve ser passível sim de proteção sob o manto da propriedade privada (empresarial ou pessoal) e com reforços jurídicos relacionados às proteções dadas aos bens intelectuais até para que se evite a depreciação deste importante ativo sob a justificativa de proteção exacerbada da privacidade conforme surgem novas regulamentações sobre dados pessoais.

---

<sup>280</sup>LANDES, William M.; POSNER, Richard A. *The economic structure of intellectual property law*, cit., p. 70-222.

O processo de invenção que passa pelas etapas de descoberta, criação, melhoria no ciclo conhecido como “PDCA” exige para que ocorra o aperfeiçoamento da inovação que haja apropriação do resultado final do conhecimento gerado pelo processo, que é um ganho legítimo para aquele que empregou os esforços para inventar algo. Mesmo que isso tenha, como sempre teve, uma limitação temporal, ou seja, prazo de proteção limitado no tempo de acordo com os interesses da Sociedade em que o desenvolvimento tecnológico cumpra um papel social.

Ou seja, é preferível do ponto de vista da segurança jurídica aplicar medidas públicas que estimulem o compartilhamento do resultado com centros de pesquisa ou terceiros, como ocorre na previsão dos artigos 218 e 219 da Constituição Federal Brasileira<sup>281</sup>, com a revisão dada pela Emenda Constitucional 85/2015, da Lei de Inovação 13.243/2016 e no Decreto de Transformação Digital 9.319/2018.

Portanto, de tudo exposto, será que de fato há necessidade do requisito humano para a proteção das bases de dados? Sendo que na grande maioria das vezes a criação será empresarial e já é possível conferir proteção a direitos de personalidades da pessoa jurídica.

Mas, a grande problemática da situação complexa da indústria dos dados, reposta justamente na delimitação sobre de quem é a propriedade, e de quem é a responsabilidade. Afinal, se há oportunidades para negócios, há riscos de dois tipos: os conhecidos, onde o dever é de prevenir e não de reparar e os desconhecidos onde o dever é de precaução.

---

<sup>281</sup>Constituição Federal de 1988, Art. 218. O Estado promoverá e incentivará o desenvolvimento científico, a pesquisa, a capacitação científica e tecnológica e a inovação.

§ 1º A pesquisa científica básica e tecnológica receberá tratamento prioritário do Estado, tendo em vista o bem público e o progresso da ciência, tecnologia e inovação.

§ 2º A pesquisa tecnológica voltará-se preponderantemente para a solução dos problemas brasileiros e para o desenvolvimento do sistema produtivo nacional e regional.

§ 3º O Estado apoiará a formação de recursos humanos nas áreas de ciência, pesquisa, tecnologia e inovação, inclusive por meio do apoio às atividades de extensão tecnológica, e concederá aos que delas se ocupem meios e condições especiais de trabalho.

§ 4º A lei apoiará e estimulará as empresas que invistam em pesquisa, criação de tecnologia adequada ao País, formação e aperfeiçoamento de seus recursos humanos e que pratiquem sistemas de remuneração que assegurem ao empregado, desvinculada do salário, participação nos ganhos econômicos resultantes da produtividade de seu trabalho.

§ 5º É facultado aos Estados e ao Distrito Federal vincular parcela de sua receita orçamentária a entidades públicas de fomento ao ensino e à pesquisa científica e tecnológica.

§ 6º O Estado, na execução das atividades previstas no caput, estimulará a articulação entre entes, tanto públicos quanto privados, nas diversas esferas de governo.

§ 7º O Estado promoverá e incentivará a atuação no exterior das instituições públicas de ciência, tecnologia e inovação, com vistas à execução das atividades previstas no caput.

E, se devido ao risco, ocorrer um evento que cause um dano<sup>282</sup>, ele terá que ser ressarcido. A questão é que no contexto atual, em que múltiplas regras se confundem fazendo com que não haja nenhuma que seja aplicada (efeito nulo), fica difícil compreender as próprias relações entre as partes, e quem tem obrigação de fazer o que para quem. E por isso, até para a blindagem legal deste ecossistema de negócios, com aplicação de seguros, as regras precisam ficar mais claras.

Importante frisar, no caso das bases de dados, ainda mais as inseridas no cenário da internet das coisas e das cidades inteligentes, há ainda a possibilidade da ocorrência do “dano social”, que pelo artigo 144 do Código Civil, seria uma figura que não é lesiva apenas ao patrimônio material ou moral da vítima, mas atinge toda a sociedade, num rebaixamento imediato do nível de vida da população.

O resultado final da equação é que, não podendo proteger a propriedade com as medidas legais corretas, sem ter os instrumentos para se calcular as consequências, ou ainda, poder determinar quem são os responsáveis, há diretamente um impacto sobre a sinistralidade, ou seja, há uma distribuição do risco para todos. É a socialização do risco como substituto da responsabilidade civil. Logo, pode-se, em um futuro próximo, acabar dividindo a conta da inércia regulatória.

É imprescindível que se faça pelo menos uma declaração de compromisso para proteção dos recursos naturais digitais essenciais para sustentabilidade da “sociedade digital” (natural digital essential *resources*), entre eles, a proteção das bases de dados.

Poderia a Conferência de Haia assumir o papel de harmonizar e unificar o tema das bases de dados? Trata-se de uma organização intergovernamental composta por mais de 60 estados-membros que se reúnem periodicamente para a negociação de tratados com o objetivo geral de “unificação progressiva do direito internacional privado.”

Não se quer repetir um novo Código de Bustamente para o meio digital, mas por certo, tendo em vista que a doutrina desempenha um papel relevante para a prática do direito internacional privado, espera-se que o presente estudo possa servir de sustentáculo acadêmico para as demandas de regulação das relações jurídicas, que geram efeitos em mais

---

<sup>282</sup>Dano é a lesão a um interesse juridicamente tutelado. Abrange, portanto, características extrapatrimoniais. Por isso temos: dano moral, dano estético, dano material, dano social. Conforme o artigo 944 do Código Civil Brasileiro a indenização se mede conforme a extensão do dano. Logo ele possui duas naturezas: compensatória e punitiva. Com a ideia de prevenção e precaução.

de um país nos temas das novas tecnologias e com o crescimento da relevância das bases de dados como um recurso essencial para a “sociedade digital”.

Ou poderia o Instituto de Direito Internacional (IDI), assumir o papel de promover a formulação de princípios gerais sobre esta matéria, considerando os objetivos do Instituto? Para o desenho de uma *Soft Law* que pudesse orientar os juristas na prática internacional do assunto que é tão complexo, multifacetado e recheado de particularidades transnacionais. Afinal, nos últimos anos o IDI tem se dedicado a publicar diversas Resoluções<sup>283</sup> com a finalidade de apoiar a uniformização do direito privado internacional.

Ou, ainda, esta tarefa poderia ser encampada pelo Instituto Internacional para Unificação do Direito Privado (UNIDROIT) ou a Comissão das Nações Unidas para o Direito Comercial Internacional (UNCITRAL), por certo, qualquer um desses organismos internacionais teriam completa competência para conduzir o encaminhamento desta pauta mais adequadamente do que apenas a tutela nacional dos Estados, tendo em vista a natureza internacional da Internet.

Segundo leciona Maristela Basso:

[...] a interpretação constitucional do DIPr também serve à identificação e constatação do pluralismo dos direitos civis nos ordenamentos nacionais. Com isso, se pode garantir em DIPr o respeito pelas mais variadas fontes de direito e a coexistência de normas de diferentes ordenamentos que disciplinam fatos revestidos de conexão transacional e geradores de efeitos territoriais e extraterritoriais imediatos.<sup>284</sup>

Qualquer proposta de autorregulamentação deve envolver: participação voluntária; as regras devem ser desenvolvidas em conjunto com os membros do setor produtivo (da indústria) para que sejam mais eficazes e haja um compromisso maior do seu cumprimento; deve haver um canal direto de denúncias para reportar infrações às regras e ser aplicado um modelo de solução de controvérsias adequado (ADRs).

Segundo o entendimento de Chris Reed<sup>285</sup>, a natureza transfronteiriça da internet traz dois tipos de desafios para a construção de qualquer regulamentação, especialmente sobre bases de dados: (i) leis nacionais que controlem a forma como se lida com a informação no tocante à informação como um bem patrimonial (propriedade), ou como um dado pessoal se

---

<sup>283</sup>Exemplo de Resolução do IDI: Resolução II sobre o conflito de leis em matéria comercial, adotada na Sessão de Turim de 12 de setembro de 1882.

<sup>284</sup>BASSO, Maristela. *Curso de direito internacional privado*, cit., p. 24.

<sup>285</sup>REED, Chris. *Internet law: text and materials*, cit., p. 308.

torne menos significativa e relevante ou mesmo impossível de se fazer impor (*to enforce*); (ii) a multiplicidade de sobreposições de leis aplicáveis e jurisdições em um caso concreto faça com que ele esteja sujeito a regulamentações contraditórias ou a nenhuma regulamentação sequer.

Deve-se evitar que haja um retrocesso de estatalidade demasiada no direito internacional privado, não se deixando enganar pela atuação comunitária da Comunidade Europeia, visto que apesar de representar-se regionalmente, para questões envolvendo impactos econômicos e sociais dos fluxos de dados pela internet o fórum deveria ser multilateral, tratado em sede da Organização das Nações Unidas (ONU) ou de outro organismo internacional de mesmo alcance.

Esta tendência de europeização das regras é muito delicada, assim como também a bilateralização ou nacionalização do tratamento de questões de grande impacto para a comunidade internacional, visto que a propriedade intelectual está dentro dos direitos humanos e demonstrou que os dados são um recurso essencial para a “sociedade da informação” do século XXI assim como foi a água para a sociedade pós-industrial.

A universalidade dos intercâmbios transfronteiriços através dos meios digitais exige um tratamento especial, princípios novos, regras atualizadas e debatidas em um fórum internacional e uma dinâmica para solução de controvérsias mais adequada do que a aplicação da regra de conexão *lex fori* e o uso dos tribunais locais.

Por certo, há uma legítima preocupação com a esfera concorrencial dentro desta dinâmica dos fluxos internacionais de dados e das trocas dos bens intelectuais sem fronteiras, como leciona Luis Silva Morais:

Atendendo à latitude dos problemas potenciais em causa, tal Inquérito será também uma componente muito sensível deste conjunto de iniciativas tendentes ao esforço do “Mercado Único Digital para a Europa”, até porque os grupos empresariais que serão predominantemente visados serão grandes grupos atuando no universo da internet oriundos dos EUA [...] não tendo sido até o presente especialmente visados pelas normas *antitrust* norte-americanos, *maxime* em matéria de ‘*monopolization*’ que representa de alguma forma o paralelo normativo, embora com certos limites, ao regime de abuso de posição dominante em sede de direito concorrencial da UE).<sup>286</sup>

---

<sup>286</sup>MORAIS, Luis Silva. Sociedade da Informação, mercados digitais, direito de autor e concorrência – É chegada a hora de uma grande reforma europeia? In: VICENTE, Dario Moura et al. *Estudos de Direito Intelectual em homenagem ao Prof. Dr. José de Oliveira Ascensão: 50 anos de vida universitária*. Coimbra: Almedina, 2016. p. 395.

Por isso, é de se entender o motivo pelo qual a proteção deve vir pelo direito internacional, pois a via local não é suficiente. Faz todo o sentido a aplicação dos princípios trazidos por TRIPs para resolver as questões da propriedade intelectual digital.

Em esclarecedora síntese Maristela Basso explica a importância destes princípios, que surgem desde GATT, com CUP e CUB, passando por TRIPs e chegando no Patent Cooperation Treat – OMPI (PCT), dentre eles: tratamento nacional<sup>287</sup>; independência dos registros, nação mais favorecida, proteção mínima (*single undertake*), esgotamento internacional de direitos (exaustão), transparência, cooperação internacional mútua, patenteabilidade absoluta, interpretação evolutiva, licença compulsória). Toda a lógica do sistema internacional é pela cooperação dos Estados-Membros, especialmente fora dos limites dos seus territórios. É este o verdadeiro incentivo para integrarem o modelo de constelação das Nações Unidas. No contexto econômico do século XX e XXI cooperação e integração se tornaram fenômenos extremamente necessários<sup>288</sup>.

Da mesma forma, Maristela Basso complementa explicando que os Estados-Partes desde GATT 1994 reconhecem como absolutamente necessário o estabelecimento de padrões e princípios adequados relativos à existência, abrangência e exercício de direitos de propriedade intelectual relacionados ao comércio e a implementação de meios eficazes e apropriados para a aplicação de normas de proteção de direitos de propriedade intelectual relacionadas ao comércio, levando em consideração as diferenças existentes entre os sistemas jurídicos nacionais, dentro de um regime de flexibilidade<sup>289</sup>

Para Miguel Reale a questão normativa envolve um árduo trabalho contínuo e evolutivo que deve acompanhar a mudança da realidade:

A tipificação normativa, não é, por conseguinte, uma obra cerebrina ou imaginosa fruto de um querer arbitrário, mas sim o resultado de uma análise positiva de dados empíricos, análise esta que culmina sempre num ato decisório, na eleição de uma dentre duas ou mais soluções possíveis. As realidades estruturais são inseparáveis de suas vias construtivas e expansivas, pois, em última análise com elas fazem corpo, sendo como são, as suas formas concretas.<sup>290</sup>

---

<sup>287</sup>GATT 477, artigos I e III; TRIPs, artigo 3,1; 4º; 6º, 63, 2, 67, 69.

<sup>288</sup>Nota de aula datada de 22.08.2016 ministrada pela Professora Maristela Basso.

<sup>289</sup>Nota de aula datada de 26.09.2016 ministrada pela Professora Maristela Basso.

<sup>290</sup>REALE, Miguel. *Direito como experiência*. São Paulo: Saraiva, 1992. p. 147.

As consequências do reconhecimento tardio de que a sociedade digital é internacional e globalizada, podem ser extremamente desastrosas e as barreiras jurídicas que estão sendo construídas agora podem se tornar intransponíveis.

Pode-se concluir, dentro de uma visão conceitual geral, que de fato, as questões envolvendo bases de dados são apropriadas para serem tratadas pelo Direito Internacional Privado, permitindo, desse modo, tratar das regras de conflitos de leis que vão necessariamente ocorrer devido a sua transnacionalidade.

Além disso, observou-se que se vem desenhando uma participação pública cada vez maior na elaboração das políticas sobre uso das bases de dados, por haver um grande interesse público envolvido e também questões relacionadas a consumidor e direito concorrencial, que justificam a intervenção mais estatal sobre o tema, não sendo pertinente seu tratamento meramente pelo direito contratualista.

De todo modo, há uma grande margem para atuação e aplicação dos contratos, principalmente no que tange a segredos de negócios, confidencialidade e proteção de dados pessoais (regras de políticas de privacidade perante parceiros e terceirizados).

Conforme ensinamentos de Leonardo Barém Leite:

[...] a evolução do tratamento jurídico conferido à pessoa jurídica, especialmente em relação aos atributos de sua personalidade, tem sensíveis reflexos na Propriedade Intelectual. Atualmente, em vista da alteração do processo criativo e de sua dinâmica, a pessoa jurídica desempenha um papel essencial na concepção de obras intelectuais que se comunicam com a sociedade.<sup>291</sup>

Nesse sentido, provavelmente uma das soluções mais rápidas e de curto prazo, seria o uso do modelo de medidas tecnológicas (como já foi feito com o *Millennium Act* e Diretiva de Fonogramas), em que se protege a confidencialidade (segredo de negócios e privacidade) com uma camada de tecnologia e há proibição de se neutralizar as medidas tecnológicas. Se não puder proteger o conteúdo das bases de dados, visto que a legislação atual só protege a sua estrutura (organização) e mesmo assim, em dois tipos de cenários, quando há originalidade (criatividade) aplica o direito autoral, e quando não há, aplica a proteção do *sui generis* (mas que não está nem harmonizada nem uniformizada, como visto).

---

<sup>291</sup>LEITE, Leonardo, Barém. O direito dos negócios e a propriedade intelectual, cit., p. 160.

No tocante às infrações, pela análise dos casos apresentados, ficariam, em princípio, melhor tratadas se aplicada o princípio *lex loci*. E onde a infração ficar muito ubíqua, devido aos desafios territoriais da ausência de fronteiras da internet, pode haver uma cláusula que determine a aplicação de *soft law* para decisão do caso, com orientação baseada nos princípios ALI ou CLIP, ou em algo novo que seja criado só para bases de dados, já que há uma tendência de haver resultados e decisões muito distintas, dependendo se for sob a ótica dos Estados Unidos ou da Europa.

Ou seja, se a possibilidade de uma articulação internacional para uma regulamentação do tipo *hard law* não estiver viável, propõe-se, ao menos, a feitura de uma *soft law* sobre cláusulas contratuais mandatórias que deveriam ser aplicadas nas relações envolvendo as bases de dados (*Mandatory clause contracts*), inspirado nos princípios CLIP e ALI, mas também na Diretiva Europeia de Cláusulas Abusivas.

Quanto a aplicação prática da tese para o Direito Brasileiro, já é mais do que chegada a hora da revisão da Lei de Direitos autorais, em vigor desde 1996, e, por certo, a questão da proteção das bases de dados merecerá especial atenção, em especial no tocante à proteção do *sui generis*, dos artigos 11, 22 e 87.

Posto isto, espera-se que a tese sirva como apoio doutrinário para futuros aprimoramentos regulatórios, ou ainda, enquanto não houver uma melhoria da lei e que as lacunas persistirem, que possa contribuir na orientação dos magistrados para tratamento mais adequado do tema nos casos concretos.

Portanto, o ideal seria propor que as bases de dados sejam tratadas como um tipo de recurso natural essencial (*natural digital resources*), para justificarem o recebimento de um tratado internacional que recaia sobre uma visão maior que apenas a discussão da propriedade, mas que seja sobre Sustentabilidade da Sociedade Digital, que está fundamentada nos pilares: garantia de fontes de energia, direito de acesso à internet (conexão) como um direito essencial, proteção das bases de dados e garantia à liberdade de informação (equilibrar todos os direitos envolvidos com o acesso e uso dos dados, patrimônio industrial, exploração econômica, confidencialidade, segredo de negócios, consumidor, concorrencial, testes dois direitos), segurança da informação.

Sem sombra de dúvida a possibilidade de poder tratar dos direitos de uso e acesso das bases de dados em um Fórum de discussão internacional para elaboração de um Tratado atualizado sobre o tema multilateral, seria a melhor solução, mais eficaz, e que pudesse,

inclusive, indicar um modelo de solução de controvérsias no modelo de ADRs, através de uma Entidade Supranacional. Mas, conforme exposto e verificado em toda a pesquisa, isso ainda exigirá um grande debate, e as demais propostas de solução podem contribuir para construir os degraus para que se chegue neste resultado final.

Isso poderia permitir melhor equilibrar todos os estes direitos envolvidos como a proteção do patrimônio industrial, o acesso e uso dos dados a sua exploração econômica, a confidencialidade, o segredo de negócios, as garantias do consumidor, a proteção da concorrência e a segurança da informação.

Neste sentido, verificou-se que a visão atual do Parlamento Europeu é a de que para o dinamismo e bom funcionamento de uma economia dos dados, é necessário permitir e proteger a circulação de dados no mercado interno europeu de modo a garantir a proteção das quatro liberdades fundamentais do mercado único da União Europeia já consagradas nos tratados (mercadorias, trabalhadores, serviços e capitais). Uma das maiores fontes de preocupação tem sido sobre a imposições de localização geográfica de dados com criação de barreiras à sua circulação.<sup>292</sup>

Ademais, há ainda as preocupações em matéria de privacidade, mas na medida que não sirvam de desculpa para restringir a livre circulação de dados de uma forma injustificada. Conforme já referido, o GDPR<sup>293</sup> prevê que em toda a UE exista um conjunto único de regras com um elevado nível de proteção dos dados pessoais. Reforça a confiança dos consumidores nos serviços em linha e assegura uma aplicação uniforme das regras em todos os Estados-Membros através de um reforço dos poderes das autoridades de proteção de dados nacionais. O GDPR promove a confiança necessária para o tratamento de dados e constitui a base para a livre circulação de dados pessoais na UE. O GDPR proíbe as restrições à livre circulação de dados pessoais no interior da União por motivos relacionados com a proteção de dados pessoais<sup>294</sup>.

---

<sup>292</sup>Fonte: PUBLIC consultation on Building the European Data Economy. *Digital Single Market*. Consultation, 10 January 2017 to 26 April 2017. Disponível em: <<https://ec.europa.eu/digital-single-market/news-redirect/52039>>. Acesso em: 24 jul. 2018.

<sup>293</sup>Regulamento 2016/679, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46 / CE (Regulamento Geral de Proteção de Dados - GDPR).

<sup>294</sup>Artigo 1.º, n. 3. Por exemplo, um endereço IP dinâmico registado por um prestador de serviços de meios de comunicação social em linha aquando da consulta por uma pessoa de um sítio Internet que esse prestador disponibiliza ao público constitui, relativamente a esse prestador, um dado pessoal, quando este último disponha de meios legais que lhe permitam identificar a pessoa em causa graças às informações suplementares que o fornecedor de acesso à Internet dessa pessoa dispõe. Ver acórdão no processo C-582/14, Breyer, ECLI:EU:C:2016:779, n.º 49.

Infelizmente, observou-se na pesquisa realizada uma tendência, tanto no lado norteamericano como europeu no sentido de uma maior localização dos dados, uma abordagem frequentemente baseada na falsa ideia de que os serviços localizados são automaticamente mais seguros do que os serviços transfronteiriços.

Além disso, o mercado de serviços de dados é influenciado em larga medida pela falta de regras transparentes e uma forte percepção da necessidade de localização dos dados. Este fator é suscetível de limitar o acesso das empresas e organizações do setor público a serviços de dados mais baratos ou mais inovadores, ou obrigar as empresas que exercem atividades transfronteiriças a providenciarem capacidades excessivas de armazenamento e tratamento de dados. Tal poderá igualmente impedir que as empresas baseadas em dados, em especial as empresas em fase de arranque, Startups e PMEs, expandam as respetivas atividades e entrem em novos mercados.

Os “dados brutos” gerados automaticamente não seriam passíveis, a uma primeira vista, pela legislação em vigor analisada, de proteção pelos direitos de propriedade intelectual vigentes, uma vez que não são considerados resultado de um esforço intelectual e/ou não têm qualquer grau de originalidade. O direito *sui generis* previsto na Diretiva relativa à proteção jurídica das bases de dados (Diretiva 96/9/CE) – que concede aos fabricantes de bases de dados o direito de impedir a extração e/ou reutilização total ou de uma parte substancial do conteúdo de uma base de dados, poderia, por sua vez assegurar uma certa proteção apenas na condição de que a criação dessa base de dados implique um investimento substancial na obtenção, verificação ou apresentação do seu conteúdo.

A Diretiva relativa à proteção de segredos comerciais (Diretiva (UE) 2016/943), poderá trazer uma camada de proteção ao segredo comercial contra a sua aquisição, utilização e divulgação ilegais. Entretanto, para que os dados sejam considerados um segredo comercial há que tomar medidas para proteger a confidencialidade das informações, que representam o capital intelectual da empresa.

Desse modo, nos termos das legislações comparadas, apenas se aplicam ações judiciais a dados se estes preencherem determinadas condições específicas para serem classificados, por exemplo, como um direito de propriedade intelectual, um direito sobre uma base de dados ou um segredo comercial.

Por conseguinte, atualmente não existem quadros políticos abrangentes quer a nível nacional ou internacional, no que se refere a dados brutos gerados automaticamente que não

se qualifiquem como dados pessoais, ou no que toca às condições da sua respectiva exploração económica. Por isso, a questão é, em grande medida, remetida para soluções contratuais.

Mas, o problema de se deixar tudo para ser governado por contratos é que este tende a um certo desequilíbrio, especialmente porque estas relações envolvem, muitas vezes, a aplicação de minutas no formato de adesão.

Ou seja, os diferentes atores do mercado que detêm o controle dos dados, em função das especificidades de cada segmento, podem, aproveitar-se de lacunas existentes no quadro regulamentar, ou das incertezas jurídicas acima descritas, impondo aos utilizadores de dados cláusulas contratuais-tipo injustas ou através de meios técnicos limitativos, como formatos próprios ou uso de cifragem.

Sendo assim, uma alternativa, seria a criação de uma regulamentação que pudesse tratar o tema dentro de um enfoque notadamente sobre o que seria considerado abusivo nos contratos relacionados a Provedores e Utilizadores de Dados (*Data Market Providers and Users*), especialmente para aplicações de IoT e de Inteligência Artificial, inspirado no precedente já realizado da Diretiva 97/7/CE e 97/13/CEE que trata sobre Cláusulas abusivas em contratos de adesão.

Por certo, a melhor alternativa seria o tratamento da matéria sobre a garantia de acesso aos dados gerados automaticamente a a proteção jurídica das bases de dados resultantes das aplicações de Inteligência Artificial (*machine learning*) dentro de uma abordagem coordenada em nível de Tratado Internacional, justamente para se evitar fragmentação país a país, ou mesmo por regiões, visto que isso seria prejudicial para o desenvolvimento da economia dos dados em termos globais, com efeitos em todos os Estados-Membros, uma vez que a Internet desde a sua concepção possui natureza internacional e transfronteiriça para fomentar um mercado de oferta de produtos e serviços globalizado.

Sendo assim, pode-se resumir algumas melhores práticas para fins de tratamento mais adequado da matéria:

- a) Tornar os bancos de dados mais criativos para aumentar a probabilidade de proteção de direitos autorais trazendo além da seleção de fatos também indicadores de análise (*analytics*) para que haja aplicação de inventividade (criatividade, originalidade);

- b) Melhorar o acesso aos dados anônimos gerados automaticamente (gerados por máquinas) através da criação de regras de partilha, reutilização e agregação;
- c) Aplicar cláusulas contratuais mais específicas para atender a necessidade de cobrir as lacunas atuais. Como por exemplo a que trata dos direitos sobre o aprendizado de máquina (*machine learning*):

**APRENDIZADO DE MÁQUINA (MACHINE LEARNING).** *A CONTRATADA é a única titular e proprietária de qualquer aprendizado sistêmico ocorrido no âmbito do Software por meio de inteligência artificial parametrizada ou neural, que compõem a base de conhecimento aprendido, resultante da aplicação de algoritmo de analytics, predição, dedução e inferência, sem que isso implique qualquer violação à direitos sobre informações confidenciais, segredos de negócios, proteção de dados pessoais relacionadas à CONTRATANTE, seus funcionários, clientes e/ou usuários, que compõem a base de dados primária.*

- d) Implementar Termos de Uso nas plataformas de dados para fins de estabelecer de forma mais clara e transparente os limites e condições de uso das bases de dados:  
*Você recebeu uma licença limitada não exclusiva e intransferível que confere direitos de uso e acesso para fins de pesquisa na plataforma online de conteúdos e repositórios digitais. Esta licença confere o direito de uso online (visualização e acesso) no formato eletrônico, por você, NÃO ESTANDO INCLUSO os direitos de reprodução, armazenamento local, impressão, captura para publicação na internet, mídias sociais ou outras plataformas digitais e/ou distribuição para terceiros, cessão ou transferência para familiares e/ou herdeiros.*
- e) Política de precificação que possa dar tratamento diferenciado aos tipos de licença conforme os tipos de direitos de uso conferidos às bases de dados;
- f) Salvaguardas tecnológicas com aplicação de medidas técnicas que possam apoiar na gestão e controle de uso e acesso das bases de dados bem como na garantia de confidencialidade (quando da necessidade da premissa de segredo de negócios ou para atender as regulamentações de proteção de dados pessoais e ciber segurança);
- g) Implementar uma abordagem não legislativa pelo caminho da autorregulamentação com adoção de recomendações de melhores praticas de normalização ISO, certificação e/ou criação de *Guidelines (Softlaw)* desenvolvidos pelo próprio mercado;

- h) Celebrar um Tratado Internacional sobre a matéria que verse sobre o tema da ética, do regime de proteções da propriedade e da responsabilidade nas aplicações de Inteligência Artificial.

Ao final, verifica-se que do ponto de vista da abordagem jurídica sobre bases de dados e sobre software, restou muito limitado o campo de visão do Direito ao comparar simplesmente com obra literária e/ou com compilações (como enciclopédias e antologias). Por certo, o nível do desenvolvimento das tecnologias digitais apresentadas tanto na percepção inovadora da Internet das Coisas (IoT) como da Inteligência Artificial, já demonstra que será necessário enfrentar novamente o assunto para trazer uma solução à altura da complexidade que se apresenta. Reduzir a análise a uma verificação de se tem ou não elementos de criatividade humana é simplificar demasiadamente do ponto de vista metodológico o que é hoje este inovador modelo de negócios que possui uma interdependência única entre as bases de dados e a solução de produto ou serviço que será ofertada à mercado.

Determinar que o registro de *copyright* ou patente será recusado se não houver uma autoria original (*original authorship*), e o que isso exatamente significa quando avançamos no uso de machine learning com algoritmos aprendizes e aplicações autônomas com assistentes conversacionais e robôs, é deixar toda a nova economia de dados e da robotização a mercê de uma imensa insegurança jurídica.

Por certo, na era da indústria 4.0, da economia do compartilhamento, da Sociedade aberta (*open society*) a aplicação do padrão da originalidade (*originality standard*) como único método não é mais condizente com a realidade atual, devendo, no mínimo, ser aplicado um método híbrido, que considera os esforços (investimentos de recursos e de tempo), e coíbe as práticas de concorrência desleal ou de abuso pelos próprios usuários (uso fora dos limites determinados pela licença).

Por certo, devem ser criados critérios para que se evite a apropriação de dados brutos, visto que isso seria o mesmo que permitir que alguém pudesse se apropriar do “oxigênio do planeta”. Lembrando que toda propriedade é sempre um regime não apenas de direitos mas de excludentes. Mas que permita, por exemplo, proteger aquele que aplica recursos para garantir a dados qualitativos com aplicação de inteligência, em analogia, seria o equivalente a proteção daquele que é capaz de produzir “água potável” (coletar, higienizar, qualificar, melhorar e entregar dentro de padrões para consumo seguro).

Por último, fica a questão do tempo de duração da proteção, qualquer que seja o tipo de direito a ser conferido para as bases de dados nas aplicações de IoT e Inteligência Artificial, qual deveria ser o tempo conferido à proteção da propriedade ou a para garantir o direito de uso e acesso aos dados? Em uma análise comparada a proposta dos Estados Unidos tem sido em torno de 25 anos (maior duração) e da União Europeia próximo dos 15 anos. Já os países nórdicos têm sugerido que não ultrapasse 10 anos dentro de uma doutrina de “apropriação indevida” (*misappropriation*). Considerando a importância de se harmonizar o livre fluxo de dados com a necessidade de retornar o investimento feito a sugestão é a de que seja pelo menor prazo possível tendendo a se equiparar ao prazo da patente devido às aplicações industriais tanto do IoT como da IA.

Acredita-se, francamente, que a melhor proposta para responder ao problema da proteção das bases de dados em um cenário de Internet das Coisas e Inteligência Artificial continue a repousar dentro da propriedade intelectual, mas, se possível, com uma abordagem mais internacional aplicando o direito dos Tratados, as medidas de salvaguarda tecnológica e o uso de um Foro de solução de controvérsias também internacional, com a possibilidade de utilização de métodos alternativos como da mediação e da arbitragem.

Para concluir, aproveito as palavras de Chris Reed, que por mais de 30 anos vem se aprofundando no estudo sobre como conseguir regulamentar a Internet, e que diz que é extremamente difícil para uma empresa ou indivíduo conseguir agir totalmente dentro da lei na Internet, quando ele se relaciona globalmente. Pois como as leis aplicáveis a internet tem escolhido a via de serem leis nacionais (locais), em algum momento ele estará infringindo alguma lei em algum lugar. E o pior, que se um dos motivos de se ter um regime legal é ter um sistema de controle de comportamento, então esta ausência de uniformidade acaba gerando justamente o contrário, a perda do controle.<sup>295</sup>

---

<sup>295</sup>REED, Chris. *Making laws for cyberspace*. United Kingdom: Oxford, 2012. Prologue, p. 8-9.

## REFERÊNCIAS

ABRÃO, Eliane Y. *Direitos de autor e direitos conexos*. São Paulo: Lumen Juris, Ebook, 2014.

ALMEIDA, Carlos Ferreira de; CARVALHO, Jorge Morais. *Introdução ao direito comparado*. 3. ed. Coimbra: Almedina, 2013

ALPA, Guido. *Da boa-fé no direito civil*. Coimbra: Almedina, 2007.

AMERICAN LAW INSTITUTE. *Intellectual property: principles governing jurisdiction, choice of law and judgments in transnational disputes*. Philadelphia, EUA: American Law Institute, 2008.

APPLE. Apple users in the EU can now download all the info the company has on them. *The Verge*, May 23, 2018. Disponível em: <<https://www.theverge.com/2018/5/23/17383692/eu-apple-users-id-privacy-portal-gdpr>>. Acesso em: 30 jun. 2018.

ARKIN, Ronald C. Ethics and Autonomous Systems: Perils and Promises. *Proceedings of the IEEE*, v. 104, n. 10, p. 1779-1781, Oct. 2016. Disponível em: <<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7571204>>. Acesso em: 24 jul. 2018.

ASCENSÃO, José de Oliveira. Bases de dados eletrônicas: o estado da questão em Portugal e na Europa. In: DIREITO da sociedade da informação. Coimbra: Ed. Coimbra, 2002. v. 3.

\_\_\_\_\_. *Concorrência desleal*. Coimbra: Almedina, 2002.

\_\_\_\_\_. *Propriedade intelectual e internet*. 2014. p. 8. Disponível em: <<http://www.fd.ulisboa.pt/wp-content/uploads/2014/12/Ascensao-Jose-PROPRIEDADE-INTELECTUAL-E-INTERNET.pdf>>. Acesso em: 10 jul. 2017.

\_\_\_\_\_. Sociedade da informação e mundo globalizado. In: WACHOWICZ, Marcos (Coord.). *Propriedade Intelectual & Internet*. 1. ed. (ano 2002), 4. tir. Curitiba: Juruá, 2005.

BARBOSA, Denis Borges. *Limites do direito de patente*. 2002. Disponível em: <<http://www.denisbarbosa.addr.com/103.rtf>>. Acesso em: 10 jul. 2017.

BARBOSA, Denis Borges. *Uma introdução à propriedade intelectual*. São Paulo: Lumen Juris, 2010.

BARLOW, John P. The economy of ideas. *Wired online*, 2 Mar. 1994. Disponível em: <<http://homes.eff.org/~barlow/EconomyOfIdeas.html>>. Acesso em: 13 jul. 2017.

BARRIUSO RUIZ, Carlos. *La contratación eletrônica*. Madrid: Dykinson, 2002.

BARROSO, Luis Roberto. A Constituição e o conflito de normas no espaço. Direito Constitucional Internacional. *Revista da Faculdade de Direito da Universidade do Estado do Rio de Janeiro*, Rio de Janeiro, n. 4, p. 201-230, 1996.

BASEDOW, Jürgen. Foundations of private international law in intellectual property. In: BASEDOW, Jürgen; KONO, Toshiyuki; METZGER, Axel (Eds.). *Intellectual property in the global arena: jurisdiction, applicable law, and the recognition of judgments in Europe, Japan and the US*. Tübingen: Mohr Siebeck, 2010.

BASSO, Maristela. *Curso de direito internacional privado*. 3. ed. São Paulo: Atlas, 2013.

BITTAR, Carlos Alberto. *Direito de autor*. 6. ed. rev. atual. e ampl. Por Eduardo C. B. Bittar. Rio de Janeiro: Forense, Ebook, 2015.

BOBBIO, Norberto. *A era dos direitos*. Tradução de Carlos Nelson Coutinho. Rio de Janeiro: Campus, 2010.

BYGRAVE, L. A. *Internet governance by contract*. 2<sup>nd</sup> ed. Oxford: United Kingdom: Oxford University Press, 2015.

CALIFORNIA passes Sweeping Law to protect online privacy. Disponível em: <<https://www.nytimes.com/2018/06/28/technology/california-online-privacy-law.html>>. Acesso em: 30 jun. 2018.

CANTNER, Uwe. Industrial dynamics and evolution – the role of innovation, competences and learning. In: DREXL, Josef; KERBER, Wolfgang; PODSZUN, Rupprecht (Eds.). *Competition policy and the economic approach: foundations and limitations*. Cheltenham, UK: Edward Elgar Publishing, 2011.

CARSON, David O. *Statement: Database and Collection of Information Misappropriation Act of 2003*. United States: United States House of Representatives – 108<sup>th</sup> Congress, 1<sup>st</sup> session, Sept. 2003.

CASIMIRO, Sofia de Vasconcelos. A proteção da informação – história de uma evolução darwiniana e da ascendência da tecnologia. In: VICENTE, Dário Moura et al. (Coords.). *Estudos de Direito Intelectual em homenagem ao Prof. Dr. José de Oliveira Ascensão: 50 anos de vida universitária*. Coimbra: Almedina, 2016.

CASTELLS, Manuel. *A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade*. Tradução de Maria X. De A. Borges. Rio de Janeiro: Jorge Zahar, 2013.

\_\_\_\_\_. *The rise of the network society*. 2<sup>nd</sup> ed. Oxford: Blackwell, 2001. (The information age: economy, society, and culture; v. 1). Disponível em: <[https://detrterritorialinvestigations.files.wordpress.com/2015/03/manuel\\_castells\\_the\\_rise\\_of\\_the\\_network\\_societybookfi-org.pdf](https://detrterritorialinvestigations.files.wordpress.com/2015/03/manuel_castells_the_rise_of_the_network_societybookfi-org.pdf)>. Acesso em: 10 jun. 2017.

\_\_\_\_\_. *A sociedade em rede: a era da informação*. Tradução de Roneide Venâncio Majer. 10. ed. São Paulo: Paz e Terra, 2007.

CEROY, Frederico Meinberg. Os conceitos de dados pessoais. *Jota*, 07 nov. 2017. Disponível em: <<https://www.jota.info/opiniao-e-analise/artigos/os-conceitos-de-dados-pessoais-07112017>>. Acesso em: 10 mar. 2018.

CHEONG, Lai Kuan; CHANG, Vanessa. The need for Data Governance: a case study. *ACIS 2007 Proceedings*, 2007. P. 1000. Disponível em: <<https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1110&context=acis2007>>. Acesso em: jul. 2018.

CHINELLATO, Silmara Juny de Abreu. Norma técnica, direito de autor e direito do consumidor. In: MORATO, Antonio Carlos; NERI, Paulo de Tarso (Orgs.). *20 anos do Código de Defesa do Consumidor: estudos em homenagem ao Professor José Geraldo Brito Filomeno*. São Paulo: Atlas, 2010.

CHWAB, Klaus; DAVIS, Nicholas. *Aplicando a Quarta Revolução Industrial*. Tradução: Daniel Moreira Miranda. São Paulo: Edipro, 2018.

COLLINS, Katie. That smart doll could be a spy. Parents, smash! *CNET Magazine*, Feb., 2017. Disponível em: <<https://www.cnet.com/news/parents-told-to-destroy-connected-dolls-over-hacking-fears/>>. Acesso em: jun. 2018.

COMMISSION launches GEAR 2030 to boost competitiveness and growth in the automotive sector. *Growth: Internal Market, Industry, Entrepreneurship and SMEs*, European Commission, 26/01/2016. Disponível em: <[http://ec.europa.eu/growth/tools-databases/newsroom/cf/itemdetail.cfm?item\\_id=8640](http://ec.europa.eu/growth/tools-databases/newsroom/cf/itemdetail.cfm?item_id=8640)>. Acesso em: 23 jul. 2018.

CONSELHO NACIONAL DE JUSTIÇA. Disponível em: <<http://www.cnj.jus.br/busca-atos-adm?documento=2579>>.

DAVIES, Ron. *The Internet of Things – opportunities and challenges*. European Parliament Research Service (EPRS), 2016. Disponível em: <[http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/557012/EPRS\\_BRI%282015%29557012\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/557012/EPRS_BRI%282015%29557012_EN.pdf)>. Acesso em: jul. 2018.

DAVISON, Mark. *The legal protection of databases*. Cambridge: Cambridge University Press, 2003. p. 293. Disponível em: <<https://books.google.com.br/books?isbn=1139435655>>. Acesso em 23 jul. 2017.

DETERMANN, Lothar. *Determann's field guide to data privacy law: international corporate compliance*. 2<sup>nd</sup> ed. Cheltenham, UK: Edward Elgar Publishing, 2015. (Elgar Practical Guides).

DIAS, Roberto. Avanços tecnológicos têm se mostrado silenciosos, impactantes e pouco visíveis. *Folha de S. Paulo*, dez, 2017. Disponível em: <<http://www1.folha.uol.com.br/cenarios/2017/12/1943494-avancos-tecnologicos-tem-se-mostrado-silenciosos-impactantes-e-pouco-visiveis.shtml?mobile>>. Acesso em: 10 mar. 2018.

DOCTOROW, Cory. *Information doesn't want to be free: laws for the internet age*. San Francisco, US: McSweeney's, 2015.

DOMINGOS, Pedro. *O Algoritmo Mestre*. São Paulo: Novatec, 2015.

DREXL, Josef et al. *Data ownership and access to data*. Position statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the Current European Debate. Disponível em: <[http://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/positionspaper-data-eng-2016\\_08\\_16-def.pdf](http://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/positionspaper-data-eng-2016_08_16-def.pdf)>. Acesso em: 10 fev. 2017.

DRIVERS Privacy Protection Act (DPPA). *What is the Driver's Privacy Protection Act (DPPA)?* Disponível em: <<https://dmv.ny.gov/drivers-privacy-protection-act-dppa>>.

DRUMMOND, Victor Gameiro. Os privilégios monopolistas como elementos comuns para os sistemas de *Copyright* e de *Droit d'auteur* e o déficit filosófico do direito de autor. In: VICENTE, Dário Moura et al. (Coords.). *Estudos de Direito Intelectual em homenagem ao Prof. Dr. José de Oliveira Ascensão: 50 anos de vida universitária*. Coimbra: Almedina, 2016.

EARLY, Chas. All new cars must contain emergency 'black boxes' by 2018, says EU. *BT.com*, Apr. 30 2015. Disponível em: <<http://home.bt.com/lifestyle/motoring/motoring-news/all-new-cars-must-contain-emergency-black-boxes-by-2018-says-eu-11363978335138>>. Acesso em: 29 jun. 2017.

EDELMAN, Benjamin G.; LUCA, Michael. *Digital discrimination: the Case of Airbnb.com*. *Harvard Business School Working Paper*, 28 Jan. 2014. Disponível em: <<https://hbswk.hbs.edu/item/digital-discrimination-the-case-of-airbnb-com>>. Acesso em: 23 jul. 2018.

ESTÚDIO ABC. Conheça 3 cidades inteligentes pelo mundo. *Exame*, 07 jul. 2017. Disponível em: <<https://exame.abril.com.br/tecnologia/conheca-3-cidades-inteligentes-pelo-mundo/>>. Acesso em: jul. 2018.

EU-Lex. *Commission Staff Working Document Advancing the Internet of Things in Europe Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Digitising European Industry Reaping the full benefits of a Digital Single Market*. SWD/2016/0110 final. Disponível em: <<https://ec.europa.eu/digital-single-market/en/news/staff-working-document-advancing-internet-things-europe>>. Acesso em: 23 jul. 2018.

\_\_\_\_\_. *Commission Staff Working Document on the free flow of data and emerging issues of the European data economy Accompanying the document Communication Building a European data economy*. (COM(2017) 9 final. Disponível em: <<https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A52017SC0002>>.

EUROPEAN COMMISSION. *Black Boxes/In-Vehicle Data Recorders*. Brussels. Disponível em: <[https://ec.europa.eu/transport/road\\_safety/specialist/knowledge/esave/esafety\\_measures\\_known\\_safety\\_effects/black\\_boxes\\_in\\_vehicle\\_data\\_recorders\\_en](https://ec.europa.eu/transport/road_safety/specialist/knowledge/esave/esafety_measures_known_safety_effects/black_boxes_in_vehicle_data_recorders_en)>. Acesso em: 28 jun. 2017.

EUROPEAN COMMISSION. *Building a European Data Economy*. Disponível em: <[https://eur-lex.europa.eu/content/news/building\\_EU\\_data\\_economy.html](https://eur-lex.europa.eu/content/news/building_EU_data_economy.html)>. Acesso em: 24 jul. 2017.

\_\_\_\_\_. Cross-border data flow in the Digital Single Market: data location restrictions. *Report / Study*, 10 Jan. 2017. Disponível em: <<https://ec.europa.eu/digital-single-market/news-redirect/51708>>. Acesso em: 24 jul. 2017.

\_\_\_\_\_. Facilitating cross border data flow in the Digital Single Market. *Report / Study*, 10 Jan. 2017. Disponível em: <<https://ec.europa.eu/digital-single-market/news-redirect/51704>>. Acesso em: 24 jul. 2017.

EUROPEAN COPYRIGHT SOCIETY. *General Opinion on the EU Copyright Reform Package*, 24 Jan. 2017. Disponível em: <<https://europeancopyrightsocietydotorg.files.wordpress.com/2015/12/ecs-opinion-on-eu-copyright-reform-def.pdf>>. Acesso em: 10 jul. 2017.

FACCIONI FILHO, Mauro. *Internet das coisas*. Palhoça: UnisulVirtual, Livro Digital, 2016.

FEDERAL COMMUNICATIONS COMMISSION. *Restoring Internet Freedom*. Disponibilidade em: <<https://www.fcc.gov/restoring-internet-freedom>>. Acesso em: 1 jun. 2017.

FERRETTI, Alessandro; PRIMICERI, Salvatore; SPEDICATO, Annalisa. *Rivoluzione d'autore: il diritto d'autore tra presente e futuro*. Primiceri Editore, 2015.

FINKELSTEIN, Claudio. E-lex mercatoria. *Revista de Direito Internacional e Econômico*, ano 3, n. 11, p. 99-106, abr./jun. 2005.

FORMAL sitting – Estonia. *Toomas Hendrik Ilves, President of the Republic of Estonia*. 2 Febr. 2016. Strasbourg. European Parliament. Disponível em: <<http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20160202+ITEM-005+DOC+XML+V0//EN>>. Acesso em: 23 jul. 2018.

FRANCO, Karin Klemp. Propriedade intelectual e ADRs no Brasil: algumas considerações sobre arbitragem, conciliação e mediação. In: *A PROPRIEDADE intelectual no novo milênio: ASPI 30 anos*. 1. ed. São Paulo: ASPI, 2013.

FRESHFIELDS BRUCKHAUS DERINGER. *Automated driving*. Germany, June 21, 2017. Disponível em: <<https://www.freshfields.com/en-gb/our-thinking/campaigns/digital/internet-of-things/connected-cars/automated-driving-law-passed-in-germany/>>. Acesso em: 01 jul. 2017.

FREUND, Fabiana Ferreira et al. Novos negócios baseados em internet das coisas. *Revista FAE*, v. 1, p 12-13, 2016.

FUNDAÇÃO GETÚLIO VARGAS. O que é uma cidade inteligente? *FGV Projetos*, 2015. Disponível em: <<https://fgvprojetos.fgv.br/noticias/o-que-e-uma-cidade-inteligente>>. Acesso em: jul. 2018.

GARNICA, L. A. *Transferência de tecnologia e gestão da propriedade intelectual em universidades públicas no Estado de São Paulo*. 2007. Dissertação (Mestrado em Engenharia de Produção) - Universidade Federal de São Carlos, São Carlos, 2007. Disponível em: <<https://repositorio.ufscar.br/bitstream/handle/ufscar/3565/DissLAG.pdf?sequence=1>>. Acesso em: 26 jan. 2018.

GEMA. Represents the copyright of mote 70,000 members in Germany. Disponível em: <<https://www.gema.de/en/>>. Acesso em: 09 jul. 2017.

GIBSON, William. *Neuromancer*. São Paulo: Aleph, 1984.

GINSBURG, Jane C. The author's place in the future of copyright. Ruth Okediji, ed., *Copyright in an Age of Exceptions and Limitations*, Cambridge University Press, 2015; Columbia Law and Economics Working Paper No. 512. *Social Science Research Network (SSRN)*. Disponível em: <<https://ssrn.com/abstract=2574496>>. Acesso em: 10 jul. 2017.

\_\_\_\_\_; GORMAN, Robert A. *Copyright law*. New York: Thomson Reuters, Ebook, 2012.

\_\_\_\_\_; TREPPOZ, Edouard. *International Copyright law: US and EU perspectives: texts and cases*. Cheltenham, UK: Edward Elgar Publishing, 2015.

GIRON, Luís Antônio. Manuel Castells: a mudança está na cabeça das pessoas. *Época*. Ideias, 11.10.2013. Disponível em: <<http://epoca.globo.com/ideias/noticia/2013/10/bmanuel-castellsb-mudanca-esta-na-cabeca-das-pessoas.html>>. Acesso em: 10 jul. 2017.

GOLDMAN, Eric. *Internet law: cases & materials*. Santa Clara University, 2016.

GOOGLE. *Information Google collects | Google Privacy Policy*. Disponível em: <<https://youtu.be/YlmVKT3Zvhw>>. Acesso em: 20 maio 2018.

\_\_\_\_\_. *Política de Privacidade do Google*. Disponível em: <<https://policies.google.com/privacy/update?hl=pt-BR>>. Acesso em: 20 abr. 2018.

GUARIZI, Débora Deflim; OLIVEIRA, Eliane Vendramini. Estudo da inteligência artificial aplicada na área da saúde. *Colloquium Exactarum*, v. 6, n. esp., p. 26-37, dez. 2014.

HAHN, J. Rizzo. Saiba o que é a Indústria 4.0 e descubra as oportunidades que ela gera. *SEBRAE Nacional*, 2016. Disponível em: <<http://www.sebrae.com.br/sites/PortalSebrae/artigos/saiba-o-que-e-a-industria-40-e-descubra-as-oportunidades-que-ela-gera,11e01bc9c86f8510VgnVCM1000004c00210aRCRD>>. Acesso em: jul. 2018.

HOBSBAWM, Eric J. *Da Revolução Industrial inglesa ao Imperialismo*. Rio de Janeiro: Forense-Universitária, 1983.

HOWKINS, John. *The creative economy*. São Paulo: Ed. Mbooks, 2012.

IMPLEMENTING the EU Copyright Directive. 2001. Disponível em: <<http://www.fipr.org/copyright/guide/eucd-guide.pdf>>. Acesso em: 10 jul. 2017.

JAYME, Erik. Considérations historiques et actuelles sur la codification du droit international privé. *Recueil des Cours de L'Académie de Droit International*, Nijhoff, Leiden, t. 177, p. 9-102, 1982. Disponível em: <<file:///C:/Users/Leonice/Downloads/67935-89367-1-PB.pdf>>. Acesso em: 05 jun. 2017.

JESSUP, Philip. *Conflicts of law. Transnational law*. New Haven: Yale University Press, 1956. p. 1. Disponível em: <<http://iglp.law.harvard.edu/wp-content/uploads/2014/10/IELR-3-Jessup-Transnational-Law.pdf>>. Acesso em: 12 maio 2017.

KERBER, Wolfgang. Competition, innovation and maintaining diversity through competition law. In: DREXL, Josef; KERBER, Wolfgang; PODSZUN, Rupprecht (Eds.). *Competition policy and the economic approach: foundations and limitations*. Cheltenham, UK: Edward Elgar Publishing, 2011.

\_\_\_\_\_. *A new (intellectual) property right for non-personal data? An Economic Analysis*. Marburg, 2016. Disponível em: <<http://www.uni-marburg.de/fb02/makro/forschung/magkspapers>>. Acesso em: 10 jun. 2017.

KLEIN, David A. *A gestão estratégica do capital intelectual*. Rio de Janeiro: Qualitymark, 2002.

KRANZBERG, Melvin. Technology and history: "Kranzberg's Laws". *Technology and Culture*, v. 27, n. 3, 1986.

LAFRANCE, Mary. *Global issues in copyright law*. Eagan, Minnesota: West, 2009.

LANDES, William M.; POSNER, Richard A. *The economic structure of intellectual property law*. Cambridge, Mass.; London, England: The Belknap Press of Harvard University Press, 2003.

LANDMARK PUBLICATIONS. *Cyber law: software and computer networks-contemporary decisions*. LandMark Publications, Ebook, 2015.

LEITE, Leonardo, Barém. O direito dos negócios e a propriedade intelectual. In: A PROPRIEDADE intelectual no novo milênio: ASPI 30 anos. 1. ed. São Paulo: ASPI, 2013.

LESSIG, Lawrence. *Jail time in the digital age. the new york times*, 2001. Disponível em: <<http://www.nytimes.com/2001/07/30/opinion/jail-time-in-the-digital-age.html>>. Acesso em: 10 jul. 2017.

MACHADO, Helena; MONIZ, Helena. *Base de dados genéticos forenses*. Coimbra: Coimbra: 2014.

MACHADO, Jorge. Desconstruindo a propriedade intelectual. *Observatório (OBS\*) Jornal*, v. 4, p. 245, 2008. Disponível em: <<http://obs.obercom.pt/index.php/obs/article/download/92/139>>. Acesso em: 10 jul. 2017.

MANZUETO, Cristiane dos Santos; TAVARES DIAS, Fernanda Mósca. Concorrência desleal, concorrência parasitária e aproveitamento parasitário. In: A PROPRIEDADE intelectual no novo milênio: ASPI 30 anos. 1. ed. São Paulo: ASPI, 2013.p. 187.

MARQUES, J. P. Remédio. Propriedade intelectual e interesse público. *Boletim da Faculdade de Direito da Universidade de Coimbra*, Coimbra, v. 79, p. 293-354, 2003.

MCCRUDDEN, Christopher. What does it mean to “compare”, and what should it mean? 2017. In: BESSON, Samantha; URSCHELER, Lukas Heckendorn; JUBÉ, Samuel (Eds.). *Comparing comparative law*. Genève: Schulthess, 2017.

MEDEIROS, Heloísa Gomes. Propriedade intelectual na sociedade informacional: produção e proteção de bens imateriais em tempos de capitalismo cognitivo. *Publica Direito*, 2014. Disponível em: <<http://www.publicadireito.com.br/artigos/?cod=7c2af8b8038c80b6>>. Acesso em: 18 jul. 2017.

METCALFE, Bob. *Internet collapses and other infoworld punditry*. IDG Books, 2000.

METZ, Rainer; BINDING Jörg; HAIFENG Pan; HUBER, Florian (Eds.). *Consumer data protection in Brazil, China and Germany*. Göttingen: Göttingen University Press, 2016. Disponível em: <[www.oapen.org/download?type=document&docid=610409](http://www.oapen.org/download?type=document&docid=610409)>.

MICROSOFT. *Microsoft Privacy Statement*. May 2018. Disponível em: <<https://privacy.microsoft.com/en-gb/privacystatement>>. Acesso em: 20 abr. 2018.

MORAIS, Luis Silva. Sociedade da Informação, mercados digitais, direito de autor e concorrência – É chegada a hora de uma grande reforma europeia? In: VICENTE, Dario Moura et al. *Estudos de Direito Intelectual em homenagem ao Prof. Dr. José de Oliveira Ascensão: 50 anos de vida universitária*. Coimbra: Almedina, 2016. p. 395.

MORGADO, Laerte Ferreira. O cenário internacional de proteção de dados pessoais. Necessitamos de um Código Brasileiro? *Âmbito Jurídico*, Rio Grande, v. 12, n. 65, jun. 2009. Disponível em: <[http://www.ambito-juridico.com.br/site/index.php?n\\_link=revista\\_artigos\\_leitura&artigo\\_id=6336](http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=6336)>.

OHNSMAN, Alan; DRANGE, Matt. Waymo V. Uber Suit Could Become Criminal Case Following Judge's Referral To Justice Department. *Forbes Staff*, May 11, 2017. Disponível em: <<https://www.forbes.com/sites/mattdrange/2017/05/11/judge-refers-waymos-uber-lawsuit-to-justice-department-grants-partial-injunction-in-case/#fdf93d341ff3>>. Acesso em: 17 jul. 2017.

OSBORNE CLARKE LLP. *Commission Communication on “Free Flow of Data” Input from the Independent Automotive Aftermarket*. FIGIEFA - Automotive Aftermarket Distributors. Europe, 2016. Disponível em: <[https://www.figiefa.eu/wp-content/uploads/Free-Flow-of-Data-FIGIEFA-Input-2016\\_12\\_23.pdf](https://www.figiefa.eu/wp-content/uploads/Free-Flow-of-Data-FIGIEFA-Input-2016_12_23.pdf)>. Acesso em: 23 jun. 2017.

OSBORNE CLARKE LLP. *Legal study on ownership and access to data*. Final report – Study. A study prepared for the European Commission DG Communications Networks, Content & Technology. Europe Union, 2016. p. 22-24. Disponível em: <<https://publications.europa.eu/en/publication-detail/-/publication/d0bec895-b603-11e6-9e3c-01aa75ed71a1/language-en>>. Acesso em: 15 fev. 2017.

PEREIRA, Alexandre Libório Dias. Bases de dados de órgãos públicos: o problema do acesso e exploração da informação do sector público na sociedade da informação. 2002. p. 1. In: ASSOCIAÇÃO PORTUGUESA DE DIREITO INTELECTUAL. *Direito da Sociedade da Informação*. Coimbra: Coimbra Ed., 2002. Disponível em: <<https://estudogeral.sib.uc.pt/bitstream/10316/28778/1/BASES%20DE%20DADOS%20D%20%C3%93RG%20%C3%83OS%20P%20%C3%9ABLICOS.pdf>>. Acesso em: 26 jul. 2018.

\_\_\_\_\_. *Direitos de autor e liberdade de informação*. Coimbra: Almedina, 2008. p. 420.

PINHEIRO, Luís de Lima. Reflexões sobre a governação e a regulação da internet, com especial consideração da ICANN. In: VICENTE, Dário Moura et al. (Coords.). *Estudos de Direito Intelectual em homenagem ao Prof. Dr. José de Oliveira Ascensão: 50 anos de vida universitária*. Coimbra: Almedina, 2016.

POIKOLA, Antti; KUIKKANIEMI, Kai; HONKO, Harri *MyData – A Nordic Model for human-centered personal data management and processing*. Ministry of Transport and Communications, [2015]. Disponível em: <<https://www.lvm.fi/-/mydata-a-nordic-model-for-human-centered-personal-data-management-and-processing-860616>>. Acesso em: 23 jul. 2018.

POLIDO, Fabrício Bertini Pasquot; ROSINA, Mônica Steffen Guise. Free open source software and creative commons in Brazil: Mapping the legal framework of alternative intellectual property licenses: In: METZGER, Axel (Ed.). *Free and open source software (FOSS) and other Alternative License Models: a comparative analysis*. Springer International Publishing, 2015.

POSNER, Richard A. *How judges think*. London-UK: Harvard University Press, 2008.

PROOF. Internet das coisas e seus desafios de segurança. *Proof*, 2017. Disponível em: <<https://www.proof.com.br/blog/iot-internet-das-coisas/>>. Acesso em: jun. 2018.

PUBLIC consultation on Building the European Data Economy. *Digital Single Market*. Consultation, 10 January 2017 to 26 April 2017. Disponível em: <<https://ec.europa.eu/digital-single-market/news-redirect/52039>>. Acesso em: 24 jul. 2018.

PUTZ, Jean-Luc. *Le droit d'auteur*. Promoculture-Larcier, 2013. Versão Ebook Kindle.

RAGEL SÁNCHEZ, Luis Felipe. La propiedad intelectual como propiedad temporal. In: VIDE, Rogel Carlos (Org.). *La duración de la propiedad intelectual y las obras en domino público*. Madrid: Reus, 2005.

REALE, Miguel. *Direito como experiência*. São Paulo: Saraiva, 1992.

REED, Chris. *Internet law: text and materials*. 2. ed. Cambridge University Press, 2004.

\_\_\_\_\_. *Making laws for cyberspace*. United Kingdom: Oxford, 2012.

RÊGO, Bergson Lopes. *Gestão e governança de dados: promovendo os dados como ativo de valor nas empresas*. Rio de Janeiro: Brasport, 2013.

REIMANN, Mathias; ZIMMERMANN, Reinhard. *The Oxford handbook of comparative law*. Oxford-UK: Oxford University Press, 2006.

RICKETSON, Sam; GINSBURG, Jane. *International copyright and neighboring rights: the Berne Convention and Beyond*. Oxford University Press, 2006.

RISH, Michael. Everything is patentable. *Tennessee Law Review*, v. 75, 2008.

RODRIGUES JR., Edson Beas. Reprimindo a concorrência desleal no comércio eletrônico: links patrocinados, estratégias desleais de marketing, motores de busca na internet e violação aos direitos de marca. *Revista dos Tribunais*, São Paulo, v.104, n. 956, p. 35-93, nov. 2015.

RUSSEL, Stuart J.; NORVIG, Peter. *Artificial Intelligence: a modern approach*. Prentice Hall, 1995. Disponível em: <<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.259.8854&rep=rep1&type=pdf>>.

SASSEN, Saskia. The global city: introducing a concept. *Brown Junior of World Affairs*, v. 11, n. 2, p. 27-43, 2005. Disponível em: <<http://www.saskiasassen.com/pdfs/publications/the-global-city-brown.pdf>>. Acesso em: 15 jul. 2017.

SIMON, Frédéric. *EU struggles for balance on free flow of business data*. *Europe*. Oct 14, 2016. Disponível em: <<https://www.euractiv.com/section/innovation-industry/news/eu-struggles-for-balance-on-free-flow-of-business-data/>>. Acesso em: 28 jun. 2017.

SOUZA, Thiago Arpagaus de Souza. Direitos morais autorais da pessoa jurídica: possibilidade de aplicação. In: *A PROPRIEDADE intelectual no novo milênio: ASPI 30 anos*. 1. ed. São Paulo: ASPI, 2013. p. 149-160.

STEMPEL, Jonathan. *Google, Viacom settle landmark YouTube lawsuit*. Disponível em: <<http://www.reuters.com/article/us-google-viacom-lawsuit-idUSBREA2H11220140318>>. Acesso em: 9 jul. 2017.

STERN, Robert M. *Issues and options for U.S.- Japan trade policies*. Ann Arbor, Michigan: The University of Michigan Press, 2005.

STIGLITZ, Joseph E. Economic foundations of Intellectual Property Rights. *Duke Law Journal*, v. 57, p. 1699-1700, 2008.

STOTT, Juliet. Black box car insurance: a young driver's new best friend behind the dashboard. *The Guardian*, England, March 26, 2016. Disponível em: <<https://www.theguardian.com/money/2016/mar/26/black-box-car-insurance-cuts-young-drivers-premiums>>. Acesso em: 30 jun. 2017.

SYMANTEC. Internet Security Threat Report 2018. *Symantec*, v. 23, 2018. Disponível em: <[http://images.mktgassets.symantec.com/Web/Symantec/%7B3a70beb8-c55d-4516-98ed-1d0818a42661%7D\\_ISTR23\\_Main-FINAL-APR10.pdf?aid=elq](http://images.mktgassets.symantec.com/Web/Symantec/%7B3a70beb8-c55d-4516-98ed-1d0818a42661%7D_ISTR23_Main-FINAL-APR10.pdf?aid=elq)>. Acesso em: jun. 2018.

TAPSCOTT, Don; TICOLL, David; LOWY, Alex. *Digital capital: harnessing the power of business web*. Harvard Business School Press, 2000.

TATEOKI, Victor Augusto. A proteção de dados pessoais e a publicidade comportamental. *Revista Juris UniToledo*, v. 2, n. 1, p. 65-75, jan/mar, 2017.

TURING, Alan M. Computing Machinery and Intelligence. *Mind*, v. 49, p. 433, 1950.

UBERTAZZI, Benedetta. *Exclusive jurisdiction in intellectual property*. Heidelberg, DE: Mohr Siebeck, 2012.

UNIÃO EUROPEIA. Conselho Europeu da União Europeia. *Mercado único digital na Europa*. Disponível em: <<http://www.consilium.europa.eu/pt/policies/digital-single-market-strategy/>>. Acesso em: 10 jul. 2017.

UNIÃO INTERNACIONAL DE TELECOMUNICAÇÕES. ‘Internet das coisas’ pode levar países emergentes a superar desafios de desenvolvimento, aponta ONU. *Nações Unidas do Brasil*, jan. 2016. Disponível em: <<https://nacoesunidas.org/internet-das-coisas-pode-levar-paises-emergentes-a-superar-desafios-de-desenvolvimento-aponta-onu/>>. Acesso em: jul. 2018.

UNITED KINGDOM. *Consumer Rights Act 2015*. Parliament: 24th Mar. 2015. Disponível em: <[http://www.legislation.gov.uk/ukpga/2015/15/pdfs/ukpga\\_20150015\\_en.pdf](http://www.legislation.gov.uk/ukpga/2015/15/pdfs/ukpga_20150015_en.pdf)>. Acesso em: abr. 2018.

UNITED STATES OF AMERICA. The national artificial intelligence research and development strategic plan. National Science and Technology Council. Networking and Information Technology Research and Development Subcommittee. Oct. 2016. Disponível em: <[https://www.nitrd.gov/PUBS/national\\_ai\\_rd\\_strategic\\_plan.pdf](https://www.nitrd.gov/PUBS/national_ai_rd_strategic_plan.pdf)>. Acesso em: 24 jul. 2018.

U.S. PATENT AND TRADEMARK OFFICE. *U. S. Patent Classification System – Classification definitions: Class 706*. U.S. Patent and Trademark Office, 2000. Disponível em: <<https://www.uspto.gov/web/offices/ac/ido/oeip/taf/def/706.htm>>. Acesso em: jul. 2018.

VAZ, Isabel. *Direito econômico da concorrência*. Rio de Janeiro: Forense, 1993.

VICENTE, Dário Moura. *A tutela internacional da propriedade intelectual*. Coimbra: Almedina, 2008.

\_\_\_\_\_; VIEIRA, José; PEREIRA, Alexandre; CASIMIRO, Sofia; SILVA, Ana (Coords.). *Estudos de direito intelectual em homenagem ao Prof. Doutor José de Oliveira Ascensão*. Coimbra: Almedina, 2016.

WACHOWICZ, Marcos. *A proteção jurídica das bases de dados em face da revolução da tecnologia da informação*. 2005. Disponível em: <<http://www.gedai.com.br/sites/default/files/arquivos/artigo-base-dados-marcos-wachowicz.pdf>>. Acesso em: 13 jun. 2017.

WEBER, Rolf H. Governance of the internet of things – from infancy to first attempts of implementation? *Laws*, v. 5, n. 3, p. 5, Jun. 2016. Disponível em: <<http://www.mdpi.com/2075-471X/5/3/28/htm>>. Acesso em: abr. 2018.

\_\_\_\_\_. Internet of Things – new security and privacy challenges. *Computer Law & Security Review*, v. 26, p. 27, 2010.

\_\_\_\_\_. Proliferation of 'Internet Governance' (September 1, 2014). GigaNet: Global Internet Governance Academic Network, Annual Symposium 2014. p. 3-4. *Social Science Research Network (SSRN)*. Disponível em: <[https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2809874](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2809874)>. Acesso em: abr. 2018.

WORLD BANK GROUP. *World Development Flagship Report 2016: Digital Dividends*. Washington DC, 2016. Disponível em: <<http://documents.worldbankorg/curated/pt/896971468194972881/pdf/102725-PUB-Replacement-PUBLIC.pdf>>. Acesso em: 10 jun. 2017.

WORLD INTELLECTUAL PROPERTY ORGANIZATION - WIPO. Alternative Dispute Resolution. Disponível em: <<http://www.wipo.int/amc/en/>>. Acesso em: 07 jul. 2017.

WORLD TRADE ORGANIZATION – WTO. Essential Medicines and Health Products Information Portal. A World Health Organization resource. Disponível em: <<http://apps.who.int/medicinedocs/en/d/Jh3009ae/>>.

YUAN, Li. China gears up in artificial-intelligence race. *Wall Street Journal*, Aug. 24, 2016. Disponível em: <<https://www.wsj.com/articles/china-gears-up-in-artificial-intelligence-race-1472054254>>. Acesso em: 23 jul. 2018.

ZECH, Herbert. Data as a tradeable commodity. In: DE FRANCESCHI, Alberto (Ed.). *European contract law and the digital single market: the implications of the digital revolution*. Cambridge: Intersentia, 2016.

ZHAO, Ning. *Choice-of-law in cross-border copyright and related rights disputes: comparative inspiration for the PRC*. Ulrik Huber Institute for Private International Law, 2012. (Doctoral Series 14).

**ANEXOS**



## ANEXO A – Análise Jurisprudencial Sobre Casos Envolvendo Bases de Dados (Brasil)

### Caso 1 – Webmotors

#### Superior Tribunal de Justiça

Conteúdo Exclusivo WEB | Maio / 2012 | JRP\2012\31259

STJ - ~~AcCiv~~ 20030110899943 - j. 30/5/2012 - julgado por Flávio ~~Rostirola~~

**DIREITO CIVIL. OBRIGAÇÃO DE NÃO FAZER. SITE DE VENDA DE AUTOMÓVEIS. ACESSO E UTILIZAÇÃO DE INFORMAÇÕES SIGILOSAS DE CLIENTES PELA CONCORRENTE. DESLEALDADE CONFIGURADA.**

**Ementa Oficial:**

EMENTA|

DIREITO CIVIL. OBRIGAÇÃO DE NÃO FAZER. SITE DE VENDA DE AUTOMÓVEIS. ACESSO E UTILIZAÇÃO DE INFORMAÇÕES SIGILOSAS DE CLIENTES PELA CONCORRENTE. DESLEALDADE CONFIGURADA.

**1. Se a dinâmica dos fatos denota o desvio de finalidade praticado pela demandada, no que tange a obtenção de informações ocultas dos clientes do site de venda de automóveis concorrente e a sua antiética utilização, forçoso reconhecer a prática de concorrência desleal, nos termos do art. 195, da Lei nº 9.279/96, o que torna lícita a tutela inibitória determinada na origem.**

2. Apelação não provida. Sentença mantida.

**Órgão** 1ª Turma Cível

**Processo N.** Apelação Cível 20030110899943APC

**Apelante(s)** ~~TECNO~~WORLD TECNOLOGIA E INFORMÁTICA LTDA E OUTROS

**Apelado(s)** ~~WEBMOTORS~~ S/A

**Relator** Desembargador FLAVIO ROSTIROLA

**Revisora** Desembargadora ANA CANTARINO

**Acórdão N°** 590.967

#### ACÓRDÃO

Acordam os Senhores Desembargadores da 1ª Turma Cível do Tribunal de Justiça do Distrito Federal e dos Territórios, FLAVIO ROSTIROLA - Relator, ANA CANTARINO - Revisora, LECIR MANOEL DA LUZ - Vogal, sob a Presidência do Senhor Desembargador LÉCIO RESENDE, em proferir a seguinte decisão: **CONHECER DA APELAÇÃO, NÃO CONHECER DO AGRAVO RETIDO E NEGAR PROVIMENTO À APELAÇÃO, UNÂNIME**, de acordo com a ata do julgamento e notas taquigráficas.

Brasília (DF), 30 de maio de 2012

Certificado nº: 4F81896F000500000FAE

30/05/2012 - 19:31

**Desembargador FLAVIO ROSTIROLA**

Relator

**RELATÓRIO**

Cuida-se de **apelação** interposta pelos Requeridos, **TECNOWORLD TECNOLOGIA E INFORMÁTICA LTDA.** e **CRISTIANO CABRAL** contra a r. sentença de fls.546/550, que tramitou perante a Décima Sexta Vara Cível da Circunscrição Judiciária de Brasília/DF.

Transcrevo o relatório judicial:

*"Trata-se de ação de conhecimento, sob o rito ordinário, ajuizada por WEBMOTORS S/A em desfavor de WEBSIS TECNOLOGIA LTDA e CRISTIANO CABRAL, estando as partes devidamente qualificadas. Esclarece a autora que mantém um site cujo principal atrativo são os anúncios de compra e venda de veículos disponibilizados em suas páginas eletrônicas, além de outros anúncios de interesse do mercado automobilístico. Registra que os anúncios são precedidos da elaboração de cadastros, nos quais são inseridos os dados pessoais de seus clientes, bem como o veículo a ser comercializado ou pretendido. Acerca dos dados pessoais de seus clientes a autora garante aos interessados absoluta privacidade. Contudo, afirma que seus clientes começaram a reclamar que outro site lhes oferecia serviços idênticos, dias após anunciarem na autora. Narra que os réus navegaram no seu site de anúncios de veículos e acessaram indevidamente os dados pessoais privados de seus clientes, a despeito do zelo na elaboração dos cadastros daqueles, fato constatado mediante a inclusão de anúncios fictícios de veículos em seu site, utilizando dados pessoais de seus próprios funcionários. Objetiva a autora a condenação dos réus na obrigação de se abster de invadir os cadastros de clientes armazenados em seus bancos de dados, uma vez que a suposta prática abusiva dos réus estaria afetando a política de privacidade dos bancos cadastrais da autora, prejudicando a sua imagem comercial e financeira, com o aliciamento de clientes. Apresenta pedido de concessão de tutela antecipada (fls. 02/10, 38/40 e 47/48). Procuração, documentos e comprovante de recolhimento da custas processuais às fls. 14/34 e 41/42. A decisão de fls.50/51 concedeu a antecipação dos efeitos da tutela para determinar que os réus se abstivessem de invadir os cadastros de clientes da autora, sob pena de multa de R\$1.000,00. Às fls.59/67 os requeridos apresentam pedido de revogação da tutela antecipada, acompanhado de documentos de fls.68/100. Consta às fls. 131/141 cópia da petição do agravo de instrumento ajuizada pelos requeridos, face o deferimento da tutela antecipada. Em contestação de fls. 144/154, os réus negam a ocorrência do acesso ilegal à base de dados cadastrais dos clientes da autora e admitem a coleta das informações por meio de navegação regular na internet. Réplica de fls. 156/157. Termo de realização de audiência de conciliação à fl. 211. A decisão de fls. 262/263 afastou a preliminar de ilegitimidade passiva, evidenciou a presença das condições da ação e os pressupostos processuais, deferiu a expedição de ofício à Quarta Delegacia - Meios Eletrônicos/SP, com vistas ao envio de cópia do inquérito policial envolvendo as partes, bem assim a realização de prova pericial.*

O laudo pericial do perito do Juízo foi juntado às fls. 320/336. Foi anexado, ainda, aos autos, laudo pericial destinado a instruir ação penal que tramitava na 10ª Vara Criminal de Vitória/ES (fls.351/355). Foram apresentados questionamentos sobre as conclusões da perícia, os quais foram respondidos pelo expert às fls. 455/456. Na petição de fls. 487/488,

a autora pugnou pela produção de prova oral, o que foi deferida às fls. 489.

Por ocasião da realização da audiência de instrução e julgamento (fl. 522), a autora reiterou o pedido de oitiva de testemunhas. O réu contestou a produção de prova oral, alegando serem eles empregados da autora. A decisão de fls. 527/529, indeferiu a produção de prova oral. Desta decisão, a autora interpôs agravo retido (fls. 532/535).<sup>deveria</sup>

Ao analisar o caso, a MM. Juíza Substituta em exercício na citada Vara houve por bem julgar procedente o pedido inicial, nos seguintes termos do dispositivo sentencial, *in verbis* (fl.550):

*"Por todo o exposto, julgo PROCEDENTE o pedido para determinar que os réus se abstenham de acessar/invasão os cadastros de clientes da autora, sob pena de multa de R\$1.000,00 por cada acesso indevido. Confirmando a tutela antecipada concedida à fl. 50. Extingo a ação, com julgamento do mérito, nos termos do artigo 269, inciso I, do Código de Processo Civil (LGL\1973\5). Condeno o requerido ao pagamento das custas processuais e despesas processuais (honorários periciais) e dos honorários advocatícios, estes que fixo em R\$ 1.000,00 (mil reais), nos termos do artigo 20, § 4º do CPC (LGL\1973\5). Transitado em julgado e, não havendo requerimentos formulados pelos interessados, dê-se baixa e arquivem-se os presentes. Sentença prolatada na Unidade de Apoio Judicial".*

As **razões de apelação dos Requeridos foram apresentadas às fls.556/568**, com o respectivo preparo à fl.569. Repisa que as provas produzidas demonstrariam que a própria Autora, Web Motors, estaria divulgando os e-mails de seus clientes, razão pela qual não haveria que se falar na responsabilidade das Demandadas pela divulgação de informações supostamente sigilosas.

Afirmam que a prova pericial produzida teria comprovado a ausência da alegada invasão ao sítio eletrônico da Apelada, que *"na época do fato alegado não havia como garantir tal privacidade uma vez que os dados: nome, ~~email~~, telefone, cidade e estado do anunciante estavam disponíveis no site da apelada de forma pública, ou seja, para qualquer usuário entrar em contato conforme apontado pelo ~~perito~~"* (fl.564)

Refuta a tese de concorrência desleal, uma vez que não teria sido demonstrada a redução do faturamento da empresa Autora, sendo que a utilização das informações contidas no anúncio do site teria sido normal e regular.

Destarte, requer o provimento da apelação e, em consequência, a improcedência do pedido inicial.

Contrarrazões da parte Autora às fls.575/578.

É o relatório.

## VOTOS

### O Senhor Desembargador FLAVIO ROSTIROLA - Relator

#### (I) Do Agravo Retido de fls.532/535

De início, não conheço do agravo retido de fls.532/535, pois não cumpridos os seus requisitos, nos termos do art.523, §1º, do CPC (LGL\1973\5).

**(II) Apelação**

CONHEÇO da apelação, pois satisfeitos os seus pressupostos extrínsecos e intrínsecos de admissibilidade.

Conforme exposto no relatório, a Autora/Apelada, ~~Webmotors S/A~~, ajuizou ação ordinária objetivando a condenação dos réus na obrigação de se abster de invadir os cadastros de clientes armazenados em seus bancos de dados, uma vez que a suposta prática abusiva dos Réus estaria afetando a sua política de privacidade, prejudicando a sua imagem comercial e financeira, com o aliciamento de clientes.

Ao analisar o caso, Sua Excelência a quo entendeu configurada a prática de concorrência desleal, vindo a conceder a tutela inibitória requerida.

Em suas razões recursais, os Recorrentes/Demandados reforçam que as provas produzidas demonstrariam que a própria Autora, Web Motors, estaria divulgando os e-mails de seus clientes, razão pela qual não haveria que se falar na responsabilidade das Demandadas pela divulgação de informações supostamente sigilosas.

Afirmam que a prova pericial produzida teria comprovado a ausência da alegada invasão ao sítio eletrônico da Apelada, que *"na época do fato alegado não havia como garantir tal privacidade uma vez que os dados: nome, ~~email~~, telefone, cidade e estado do anunciante estavam disponíveis no site da apelada de forma pública, ou seja, para qualquer usuário entrar em contato conforme apontado pelo ~~perito~~"* (fl. 564)

Refuta a tese de concorrência desleal, uma vez que não teria sido demonstrada a redução do faturamento da empresa Autora, sendo que a utilização das informações contidas no anúncio do site teria sido normal e regular.

A princípio, impõe o registro que a r. sentenciante concedeu a tutela requerida na inicial não com base no acesso ao sítio eletrônico que, como demonstrado, de livre conexão a qualquer pessoa que tivesse acesso à internet, mas em razão da utilização indevida de informações pessoais dos clientes ali cadastrados, por meio ardil, com o intuito de obter o desvio de clientela.

Tais fatos ocorreram no **ano de 2003**.

Após a averiguação perante a Delegacia Civil de São Paulo/SP, apurou-se que os clientes da Autora estavam recebendo diversas mensagens indesejadas de procedência dos Recorrentes/Requeridos (fls.26/29).

Chegou-se a se instaurar o competente processo criminal para apuração dos fatos, sobretudo porque as mensagens teriam sido encaminhadas de computador vinculado ao Ministério da Saúde (setor de Assessoria de Informática do PROFAE), pelo 2º Requerido.

Igualmente, fora determinada perícia para se comprovar a existência de evidências na máquina IP 200.176.216.132 com origem dos ~~emails~~ enviados em nome do site [www.bancodeveiculos.com.br](http://www.bancodeveiculos.com.br), de responsabilidade dos Demandados.

Uma das máquinas restou prejudicada a análise, porque teve o seu disco formatado, o que atrai o forte indício de que o intuito seria o de eliminar quaisquer vestígios que pudessem

desembocar na autoria e na materialidade do delito.

A outra máquina, denominada de máquina 1, apresentava defeito, inviabilizando a coleta de novas evidências, o que veio a prejudicar na resposta de diversos outros quesitos (fls.326/327).

Em sede de cognição sumária, ao julgar o Agravo de Instrumento nº 2003.00.2.010447-4, sob a relatoria do Desembargador Fernando ~~habibe~~, essa e. Turma concluiu (fls.482/484):

*"Logo, o que se conclui, ao menos nesta sede, é que as informações não estão disponíveis à maioria dos internautas. Trata-se, antes, de informações ocultas à maioria, às quais só têm acesso quem disponha de conhecimentos mais ou menos avançados em informática. Pretendesse a agravada divulgá-las, as deixaria expostas no site para qualquer um que o visitasse. Portanto, **o simples fato das informações cadastrais não estarem aparentes quando da visualização da página de internet revela, em princípio, a clandestinidade do modo como foram obtidos pelos agravantes.** Acrescento que o prestígio e confiança conquistados pela agravada em anos de veiculação de anúncios, corroborados pela alta quantia pela qual foi vendida, demonstram que a conduta dos agravantes pode abalar sua relação com os clientes. Este fato restou demonstrado pela indignação e desconfiança de clientes que se sentiram ameaçados pela inesperada comunicação dos réus (41). Tais razões são suficientemente convincentes quanto a verossimilhança das alegações da autora e a possibilidade de danos de difícil reparação, cumprindo os requisitos autorizadores da medida previstos no CPC (LGL\1973\5) 273, traduzida, no caso, na ordem de não invadir o castro de clientes mantido pela agravada, sob pena de multa de R\$1.000,00 por cada acesso indevido".*

A par de toda essa constatação e da dinâmica dos fatos, a r. sentenciante chegou à ilação do desvio de finalidade, o que, no meu entender, revelou-se acertada, sobretudo pela obtenção de informações ocultas e a sua antiética utilização – ou no mínimo imprudente –, o que, inclusive, veio a ocasionar confusão e dúvidas entre os consumidores, hipótese configuradora da concorrência desleal, nos termos do art. 195, da Lei nº 9.279/96.

A esse respeito, o seguinte aresto desse e. Tribunal:

*"A concorrência desleal é ilícito civil em que o concorrente tanto pode agir com a consciência de que está praticando um ato contrário à concorrência correta, como pode agir de forma imprudente, sem adoção dos cuidados esperados de um comerciante normal.". (Acórdão n. 365969, 20060110983260APC, Relator LEILA ARLANCH, 4ª Turma Cível, julgado em 01/04/2009, DJ 15/07/2009 p. 19)*

Logo, nada a reparar na r. sentença, cujos fundamentos integro à presente decisão, *in verbis* (fls.548/550):

*"Como é sabido, na atualidade, um cadastro de consumidores é de muita valia, sobretudo para quem comercializa pela internet.*

A cópia do inquérito policial instaurado pela requerente contra os réus (fl.26) junto à 4ª Delegacia contra crimes eletrônicos/SP, demonstra que as mensagens indesejadas enviadas aos clientes da autora eram provenientes de computadores manejados pelos réus. Os próprios requeridos afirmam que acessaram regularmente à página da autora,

sem que tivesse havido quebra de senha, alegam, pois, não haver que se falar em invasão.

Questionam os réus que se qualquer interessado em comprar o automóvel anunciado pela requerente ou auxiliar na venda, pode acessar os dados da página eletrônica da autora porque não poderia outro fornecedor de serviço semelhante fazer o mesmo.

Entendo que o comportamento reprovável neste feito é a utilização indevida pelos réus das informações conseguidas sobre os clientes da autora, ou seja, o oferecimento pelos requeridos àqueles clientes dos mesmos serviços prestados pela requerente. Trata-se, pois, de prática abusiva que prejudica os negócios da autora. É um caso de concorrência desleal, vedada pela legislação brasileira. Nesse sentido segue o escólio de FÁBIO ULHOA COELHO: "A repressão à concorrência desleal, por sua vez, é feita em dois níveis pelo direito. Na área do direito penal, a lei tipifica como crime de concorrência desleal os comportamentos elencados no artigo 195 da LPI. São exemplos desses crimes: publicar falsamente afirmação em detrimento de concorrente, com o objetivo de obter vantagem; empregar meio fraudulento para desviar, em seu proveito ou de terceiro, a clientela de um certo comerciante; dar ou prometer dinheiro a empregado de corrente para que este proporcione vantagem, faltando o dever do emprego etc." (Manual de Direito Comercial, fl. 30). Cumpre-me salientar que a Carta Magna (LGL\1988\3), ao contrário de proibir a concorrência empresarial, eleva-a à condição de princípio constitucional, protegendo-a e estimulando-a. O que a legislação nacional veda é a concorrência feita de forma desleal, sem atender aos princípios da honestidade e correção comercial.

É certo que não existe na legislação pátria uma definição para o termo "concorrência desleal". Contudo, é de comum sabença que o ato de concorrência desleal importa numa apreciação de fato, sujeita ao exame do caso concreto que se coloca à frente do julgador, quando afrontados os conceitos abertos de lealdade, bons costumes, usos e costumes honestos no comércio.

A meu sentir, na hipótese vertente estão presentes todos os elementos aptos a configurar a prática pelos réus de concorrência desleal, mediante captação indevida de clientela, o que provoca dano patrimonial à requerente. In casu, portanto, a irrisignação da autora merece prosperar para que os réus se abstenham de invadir/acessar os cadastros de clientes armazenados em seus bancos de dados".

Ante o exposto, não conheço do agravo retido e **NEGO PROVIMENTO à apelação** dos Requeridos, mantendo-se indene a r. sentença hostilizada.

É o meu voto.

**A Senhora Desembargadora ANA CANTARINO - Revisora**

Com o relator.

**O Senhor Desembargador LECIR MANOEL DA LUZ - Vogal**

Com o Relator.

#### **DECISÃO**

CONHECER DA APELAÇÃO, NÃO CONHECER DO AGRAVO RETIDO E NEGAR PROVIMENTO À APELAÇÃO, UNÂNIME.

**Caso 2 – All Match**

**TRIBUNAL DE JUSTIÇA**  
**PODER JUDICIÁRIO**  
São Paulo



Registro: 2014.0000438799

**ACÓRDÃO**

Vistos, relatados e discutidos estes autos de Apelação nº 0219056-85.2007.8.26.0100, da Comarca de São Paulo, em que são apelantes ALL MATCH PROCESSAMENTO DE DADOS LTDA e RICARDO MALAGUTI REIS e é apelada DATA SOLUTIONS SERVIÇOS DE INFORMATICA LTDA.

ACORDAM, em 1ª Câmara de Direito Privado do Tribunal de Justiça de São Paulo, proferir a seguinte decisão: "Negaram provimento ao recurso. V. U.", de conformidade com o voto do Relator, que integra este acórdão.

O julgamento teve a participação dos Exmos. Desembargadores CHRISTINE SANTINI (Presidente sem voto), PAULO EDUARDO RAZUK E RUI CASCALDI.

São Paulo, 29 de julho de 2014.

**Luiz Antonio de Godoy**  
Relator  
Assinatura Eletrônica



TRIBUNAL DE JUSTIÇA  
PODER JUDICIÁRIO  
São Paulo

**VOTO Nº 29842**

**APELAÇÃO Nº 0219056-85.2007.8.26.0100 – São Paulo**

**APELANTE All Match Processamento de Dados Ltda. e Ricardo Malaguti Reis**

**APELADA Data Solutions Serviços de Informática Ltda.**

**JUIZA Lúcia Caninéo Campanhã**

**RESPONSABILIDADE CIVIL - Concorrência desleal - Alegação de utilização de informações confidenciais pelos réus - Titularidade dos programas da autora e seu acesso indevido por parte dos réus verificados - Corréu que deixou de prestar os serviços para a autora e tornou-se sócio da empresa requerida, passando a desenvolver atividade semelhante - Existência de alto grau de similaridade nas bases de dados das empresas, indicando que os réus utilizavam informações trazidas da autora e as atualizavam - Réus que desenvolveram seu banco de dados utilizando como base o banco de dados da autora - Multa devida, conforme estabelecido no termo de confidencialidade - Danos materiais constatados - Violação à propriedade intelectual de programa de computador - Honorários advocatícios - Redução indevida - Observância dos comandos pertinentes da lei processual - Sentença mantida - Art. 252 do RITJSP/2009 - Recurso desprovido.**

Trata-se de apelação da sentença de fls. 331/337 (objeto de embargos de declaração rejeitados a fls. 378), em que, em hipótese de "ação de indenização por violação de direito autoral e concorrência desleal" (fls. 2) ajuizada por Data Solutions Serviços de Informática Ltda. contra All Match Processamento de Dados Ltda., Ricardo Malaguti Reis e Maya Segers, foi julgada procedente em parte a demanda



TRIBUNAL DE JUSTIÇA  
 PODER JUDICIÁRIO  
 São Paulo

"para condenar o requerido Ricardo Malaguti dos Reis no pagamento de multa de R\$ 100.000,00 (cem mil reais), com correção monetária desde março de 2007 (fls. 40) e juros de 1% ao mês a partir da citação, para condenar a requerida All Match Processamento de Dados Ltda. no pagamento de indenização por danos materiais, com valor a ser fixado por arbitramento, conforme exposto no parágrafo anterior" (fls. 337) e improcedente em relação a Maya Segers. Já a medida cautelar (autos em apenso) envolvendo as mesmas partes foi julgada procedente, confirmando-se a liminar. Foram carreados aos réus All Match Processamento de Dados Ltda. e Ricardo Malaguti Reis os ônus da sucumbência. Inconformados, apelaram estes, sustentando que "o trabalho desenvolvido por Ricardo Malaguti dos Reis no âmbito das atividades da empresa Apelante All Match - Processamento de Dados Ltda. não tem qualquer correlação com o software e sistema de captura de informações noticiados pela Apelada" (fls. 349). Aduziram que o termo de confidencialidade firmado pelo réu Ricardo não teria o condão de impedir que desenvolvesse outro sistema de banco de dados. Afirmaram ausência de violação de direitos autorais. Alegaram, ainda, que não fora demonstrado nos autos a titularidade da autora quanto aos "softwares" em questão. Sustentaram inoccorrência dos alegados danos materiais. Pleitearam, por fim, eventual redução do valor da multa fixado na sentença. Foi providenciado o recolhimento do preparo. Oferecidas contrarrazões, foram os autos remetidos a este Tribunal.

É o relatório, adotado, quanto ao restante, o da sentença apelada.

Ajuizou a autora a presente demanda, pretendendo o ressarcimento das perdas e danos decorrentes da prática pelos réus de atos que configurassem concorrência desleal, em razão de suposta utilização de informações confidenciais.

Examinados os autos, é certo que a sentença combatida trouxe adequada solução à questão em debate, merecendo ser integralmente confirmada.

Como observado na sentença, "As pessoas físicas incluídas no polo passivo prestaram serviços para a autora e quando se desligaram da empresa, nos meses de fevereiro e março de 2007, firmaram compromisso declarando que



TRIBUNAL DE JUSTIÇA  
PODER JUDICIÁRIO  
São Paulo

receberam informações confidenciais relativas aos projetos, banco de dados, equipamentos, hardwares, softwares, consistentes em segredo comercial, de propriedade exclusiva da autora. Comprometeram-se a tomar as medidas necessárias para impedir que as informações confidenciais sejam copiadas, transferidas, divulgadas ou utilizadas sem a autorização da autora, tudo sob pena de multa de R\$ 100.000,00 (fls.39/40 e 46/47)./Ocorre que tão logo o requerido Sr. Ricardo deixou de prestar os serviços para a autora tomou-se sócio da empresa requerida e passou a desenvolver atividade semelhante. A empresa requerida iniciou suas atividades em 27 de abril de 2007, com data de constituição em 8 de maio de 2007 (fls.48). (...) Quando do cumprimento do mandado de busca e apreensão, os peritos constataram a violação e lacraram as CPUs para que fossem abertas posteriormente na presença dos assistentes técnicos para elaboração do laudo (fls.71 do apenso)./Constou do laudo pericial o alto grau de similaridade nos dados constantes da base de dados indicando que os réus utilizavam informações trazidas da autora e as atualizavam. Acrescentou que a grande similaridade entre os layouts das tabelas reforça tal conclusão (fls.187 do apenso)./Depois de comparar os programas, o perito concluiu que foram encontrados nos computadores dos réus cópias dos softwares "Data Setting", "Manager", "Pesquisa Receita PF/PJ" e "MQEXEC", desenvolvidos pela autora./Também verificou indícios de que os réus procediam o desenvolvimento de seu banco de dados utilizando como base o banco de dados da autora (fls.194 do apenso)./O perito esclareceu que mesmo não sendo possível executar o programa "Data Setting" com os cinco arquivos encontrados não afasta a conclusão de que localizados softwares protegidos legalmente nos computadores periciados (fls.183)./ Ressaltou o perito que a autora entregou a lista de arquivos antes do início dos trabalhos e esses arquivos foram encontrados nos computadores dos réus (fls.183), o que confirma a titularidade dos programas da autora e seu acesso indevido por parte da ré" (fls. 334/335).

É certo, também, que "é de se estranhar que uma empresa recém constituída tivesse tempo hábil para desenvolver todos os seus programas e base de



TRIBUNAL DE JUSTIÇA  
PODER JUDICIÁRIO  
São Paulo

dados em tão pouco tempo. O mais plausível é que o sócio oriundo da empresa concorrente tenha aproveitado a base de dados e os programas da empresa autora, não obstante o termo de confidencialidade firmado. Tal conclusão coaduna-se com o laudo pericial" (fls. 336).

Diante disso, constata-se ter sido corretamente condenado o corréu Ricardo Malaguti Reis no pagamento de multa no valor de R\$ 100.000,00, conforme estabelecido na "Declaração e Compromisso" (fls. 39), firmado entre ele e a autora.

Ademais, como anotado pela Juíza de Direito, "demonstrada a violação à propriedade intelectual de programa de computador de titularidade da autora, impõe-se a condenação da pessoa jurídica em perdas e danos, visto que consiste na beneficiária direta dessa violação./O valor será apurado em liquidação por arbitramento e corresponderá ao lucro líquido obtido pela ré nos serviços prestados que tenham qualquer relação com a base de dados da autora ou os programas "Data Setting" ou "Manager" ou "Pesquisa Receita PF/PJ" ou "MQEXEC" (fls. 337).

Por fim, quanto aos honorários advocatícios, não há razão para sua redução. Foram eles fixados com estrita observância dos comandos pertinentes da lei processual, tendo sido considerada a sucumbência em maior proporção dos réus. Ademais, foram levados em conta o zelo profissional, o lugar da prestação do serviço, a natureza e a importância da causa, bem como o trabalho realizado e o tempo exigido para tanto.

Assim, nos termos do art. 252, do Regimento Interno do Tribunal de Justiça do Estado de São Paulo, ratificam-se os fundamentos da sentença recorrida, ora mantida por revelar-se suficientemente motivada.

É essa, inclusive, a orientação do Superior Tribunal de Justiça:

"PROCESSUAL CIVIL. ACÓRDÃO PROFERIDO EM EMBARGOS DECLARATORIOS. RATIFICAÇÃO DA SENTENÇA. VIABILIDADE. OMISSÃO INEXISTENTE. ART. 535, II, DO CPC. AUSÊNCIA DE VIOLAÇÃO. 1.Revela-se improcedente suposta ofensa ao art. 535 do CPC quando o Tribunal de origem, ainda que não aprecie todos os argumentos expendidos pela parte recorrente, atém-se aos contornos da lide e fundamenta



**TRIBUNAL DE JUSTIÇA**  
**PODER JUDICIÁRIO**  
 São Paulo

sua decisão em base jurídica adequada e suficiente ao desate da questão controvertida. 2.É predominante a jurisprudência do Superior Tribunal de Justiça em reconhecer a viabilidade de o órgão julgador adotar ou ratificar o juízo de valor firmado na sentença, inclusive transcrevendo-o no acórdão, sem que tal medida encerre omissão ou ausência de fundamentação no decisum. 3.Recurso especial não-provido” (REsp. nº 662.272 – RS, 2ª Turma do Superior Tribunal de Justiça, v. un., Rel. Min. João Otávio Noronha, em 4/9/07, DJ de 27/9/07, pág. 248).

“CIVIL. PROCESSUAL CIVIL. ACÓRDÃO. FUNDAMENTAÇÃO. INSPIRAÇÃO. DECISÃO. ANTERIOR. POSSIBILIDADE. OMISSÃO. 1. A Corte a quo manifestou-se pela confirmação integral da sentença monocrática, ratificando todos os seus fundamentos, de modo que restou absorvido pelo aresto o fundamento de que a anterioridade deve ser observada a partir da Medida Provisória 368/93. 2. Não se configura desprovido de fundamentação, tampouco omissivo, o julgado que repete fundamentos adotados pela sentença, com sua transcrição no corpo do acórdão. Precedentes. 3. Recurso especial improvido” (REsp. nº 641.963 – ES, 2ª Turma do Superior Tribunal de Justiça, v. un., Rel. Min. Castro Meira, em 8/11/05, DJ de 21/11/05, pág. 182).

Nessas circunstâncias, nega-se provimento ao recurso.

**LUIZ ANTONIO DE GODOY**  
 Relator

*Caso 3 – JR*

PODER JUDICIÁRIO  
 TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO



Registro: 2017.0000079604

### ACÓRDÃO

Vistos, relatados e discutidos estes autos de Apelação nº 0029835-79.2013.8.26.0001, da Comarca de São Paulo, em que é apelante JR DO BRASIL COMERCIO DE FERRAMENTAS LTDA - EPP, é apelado SILVA & LOPES DO BRASIL COMERCIO DE FERRAGENS E FERRAMENTAS LTDA - EPP.

ACORDAM, em 2ª Câmara Reservada de Direito Empresarial do Tribunal de Justiça de São Paulo, proferir a seguinte decisão: "**Negaram provimento ao recurso. V. U.**", de conformidade com o voto do Relator, que integra este acórdão.

O julgamento teve a participação dos Exmos. Desembargadores CARLOS ALBERTO GARBI (Presidente), CLAUDIO GODOY E ALEXANDRE MARCONDES.

São Paulo, 13 de fevereiro de 2017.

CARLOS ALBERTO GARBI  
 -RELATOR -



PODER JUDICIÁRIO  
TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO

Apelação nº 0029835-79.2013.8.26.0001 – São Paulo (3ª Vara Cível do Foro Regional de Santana)

Apelante: Jr. do Brasil Comércio de Ferramentas Ltda - Epp

Apelada: Silva & Lopes do Brasil Comércio de Ferragens e Ferramentas Ltda - Epp

[ VOTO Nº 24.959 ]

**INDENIZAÇÃO. CONCORRÊNCIA DESLEAL. DESVIO DE CLIENTELA E FURTO DE BASE DE DADOS DE CLIENTES. NÃO COMPROVAÇÃO. IMPROCEDÊNCIA MANTIDA. RECURSO NÃO PROVIDO.**

Indenização. Alegação de concorrência desleal. Desvio de clientela e furto de base de dados de clientes da autora por sócio da ré, que foi seu funcionário. Não comprovação. Ônus da prova da autora. Provas oral e documental que não comprovaram a alegação da inicial. Improcedência mantida. Recurso não provido.

A sentença proferida pelo **Doutor Jorge Alberto Quadros de Carvalho Silva** julgou improcedente o pedido e condenou a autora ao pagamento das custas e das despesas processuais, bem como na verba honorária advocatícia sucumbencial fixada 10% sobre o valor da causa, atualizado.

A autora recorreu da sentença e alegou, sem síntese, que a empresa-ré foi constituída enquanto o seu sócio ainda era seu funcionário; que o sócio foi surpreendido abordando clientes; que a ré praticou espionagem e concorrência desleal; que houve captura não autorizada de sua base de



PODER JUDICIÁRIO  
TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO

dados de clientes; que a ré copiou seus dados; que restou caracterizada a concorrência desleal; e que procede seu pedido.

A ré apresentou resposta na qual pediu a manutenção da sentença.

**É o relatório.**

A autora alegou que seu ex-funcionário *Sivaldo de Lima Lopes* constituiu empresa na mesma área que trabalha e que praticou atos de concorrência desleal. Afirmou que a ré, que tem "*como objeto social, firma de trabalho e público alvo os mesmos clientes da requerente*" (fls. 03), desviou clientes e furtou dados internos através do sócio que até então era seu funcionário, de modo que pediu sua condenação em indenização pelos danos causados, estimada em 100 salários mínimos.

A ré negou os fatos, tendo sustentando que o ex-funcionário da autora tem demanda trabalhista contra a autora, com resultado favorável em Segunda Instância.

A autora pediu, assim, a expedição de ofício ao SENAI – Serviço Nacional de Aprendizagem Industrial e a produção da prova oral que, contudo, não comprovaram as alegações constantes na inicial.

A única testemunha ouvida na audiência de instrução e julgamento "*Não soube dizer se Sivaldo desviou clientela da autora para a empresa que montou*" (fls. 94) e da resposta ao ofício do SENAI extrai-se apenas que a ré foi constituída em data próxima à demissão do referido ex-funcionário.

A autora alegou que a ré, por meio de seu sócio, desviou clientela e



PODER JUDICIÁRIO  
TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO

furtou sua base de clientes. Essa era a comprovação que deveria ter produzido nos autos, vez que o ônus da prova lhe recaía, nos termos do art. 333, inc. I, do CPC/73, aplicável à causa. Todavia, a simples circunstância de a ré ter sido constituída em data próxima à demissão do sócio não é indicativa de que referidos atos graves e que podem, inclusive, caracterizar crime, tenham ocorrido.

A sentença acertadamente entendeu que:

“Os documentos exibidos não são suficientes para corroborar as alegações da autora, a quem cabia provar o fato constitutivo de seu direito, nos termos do artigo 373 do Código de Processo Civil.

É certo que o sócio na ré, Sivaldo, manteve vínculo empregatício com autora, de quem recebeu aviso prévio em 02.05.2011 (fls. 21). A relação de emprego entre as partes faz presumir que ele tivesse tido acesso a informações privilegiadas.

Incontestável que no mesmo mês em que foi demitido constituiu empresa com o mesmo objeto social da autora (fls. 13/14).

Porém, o simples fato da abertura dessa empresa não é suficiente para caracterizar a prática ilícita.

Com efeito, não ficou demonstrado que tivesse feito uso indevido de informações privilegiadas, denegrido a concorrente e gerado dano à autora.

O e-mail de fls. 16, de 25.05.2011, remetido à Fertools, suposta cliente da autora, bem como os documentos exibidos pelo SENAI (fls. 137/152), evidenciam tão-somente a apresentação e cadastro da ré no mercado, mas não caracterizam a concorrência desleal.

Ademais, a testemunha arrolada pela autora nada pode confirmar quanto à prática de captação ilícita de clientela (fls. 94)”



PODER JUDICIÁRIO  
TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO

Assim, não comprovado qualquer ato de concorrência desleal praticado pela ré contra a autora, não havia outra solução à lide senão a improcedência do pedido, como acertadamente a sentença julgou o pedido.

Pelo exposto, **NEGO PROVIMENTO** ao recurso, e majoro a verba honorária advocatícia sucumbencial para 15% sobre o valor da causa (art. 85, §11, NCPC).

**CARLOS ALBERTO GARBI**  
—relator—



## ANEXO B – Análise Jurisprudencial Sobre Casos Envolvendo Bases de Dados (Europa)

### *Caso 1 – Lion Laboratories*

## LION LABORATORIES LTD V EVANS: CA 1985

April 14, 2016 @ Intellectual Property,

**References:** [1985] QB 526

**Coram:** Stephenson LJ, Griffiths LJ

**Ratio** Lion Laboratories manufactured and marketed the Lion Intoximeter which was used by the police for measuring blood alcohol levels of motorists. Two ex-employees approached the Press with four documents taken from Lion. The documents indicated that the Lion Intoximeter had faults which could have resulted in a significant number of motorists being wrongly convicted. Lion started proceedings against their ex-employees and Express Newspapers Limited to restrain disclosure of the information as to the faults. They obtained an interlocutory injunction restraining breach of confidence and infringement of copyright. The defendants appealed.

Held: The Court of Appeal allowed the appeal. The documents contained confidential information it would have been a breach of confidence to publish the information in them and an infringement of copyright to publish the documents themselves unless there were defences which permitted that in the public interest.

**Ratio Stephenson LJ** The judge was ‘right to make no difference between confidence and copyright for the purposes of this case’ and ‘The problem before the judge and before this court is how best to resolve, before trial, a conflict of two competing public interests. The first public interest is the preservation of the right of organisations, as of individuals, to keep secret confidential information. The courts will restrain breaches of confidence, and breaches of copyright, unless there is just cause or excuse for breaking confidence or infringing copyright. The just cause or excuse with which this case is concerned is the public interest in admittedly confidential information. There is confidential information which the public may have a right to receive and others, in particular the press, now extended to the media, may have a right, and even a duty to publish, even if the information has been unlawfully obtained in flagrant breach of confidence and irrespective of the motive of the informer. The duty of confidence, the public interest in maintaining it, is a restriction on the freedom of the press which is recognised by our law, as well as by article 10(2) of the Convention for the Protection of Human Rights and Fundamental Freedoms (1953) (Cmd. 8969); the duty to publish, the countervailing interest of the public in being kept informed of matters which are of real public concern, is an inroad on the privacy of confidential matters.’ There were four considerations. ‘. . . The public are interested in many private matters which are no real concern of theirs and which the public have no pressing need to know. Secondly, the media have a private interest of their own in publishing what appeals to the public and may increase their circulation or the numbers of their viewers or listeners; . . . Thirdly, there are cases in which the public interest is best served by an informer giving the confidential information, not to the press but to the police or some other responsible body. . . . Fourthly . . . ‘there is no confidence as to the disclosure of iniquity’: and in 1984 extends to serious misdeeds or grave misconduct, he submits that misconduct of that kind is necessary to destroy the duty of confidence or excuse the breach of it, and nothing of that sort is alleged against the plaintiffs in the evidence now before the court.’ and ‘What makes this case so special is that the plaintiffs’ right to

keep inviolate the secrecy of the information which the defendants wish to publish is undisputed, and the only question for interlocutory decision is whether that right is outweighed by the public interest, not in exposing persons who may be guilty of offences for which they have not been punished, but in disclosing the risk of the plaintiffs being instrumental in punishing other people for offences which they may not have committed.’ ‘The issue raised by the defendants is a serious question concerning a matter which affects the life, and even the liberty of an unascertainable number of Her Majesty’s subjects and though there is no proof that any of them has been wrongly convicted on the evidence of the plaintiffs’ Intoximeter, and we certainly cannot decide that any has, we must not restrain the defendants from putting before the public this further information as to how the Lion Intoximeter 3000 has worked, and how the plaintiffs regard and discharge their responsibility for it, although the information is confidential and was unlawfully taken in breach of confidence.’

**Ratio** Griffiths LJ: ‘The first question to be determined is whether there exists a defence of public interest to actions for breach of confidentiality and copyright, and if so, whether it is limited to situations in which there has been serious wrongdoing by the plaintiffs – the so-called ‘iniquity’ rule.

I am quite satisfied that the defence of public interest is now well established in actions for breach of confidence and, although there is less authority on the point, that it also extends to breach of copyright: see by way of example *Fraser v Evans* [1969] 1 QB 349; *Hubbard v Vosper* [1972] 2 QB 84; *Woodward v Hutchins* [1977] 1 WLR 760 and *British Steel Corporation v Granada Television Ltd* [1981] AC 1096.

I can see no sensible reason why this defence should be limited to cases in which there has been wrongdoing on the part of the plaintiffs. I believe that the so-called iniquity rule evolved because in most cases where the facts justified a publication in breach of confidence, it was because the plaintiff had behaved so disgracefully or criminally that it was judged in the public interest that his behaviour should be exposed. No doubt it is in such circumstances that the defence will usually arise, but it is not difficult to think of instances where, although there has been no wrongdoing on the part of the plaintiff, it may be vital in the public interest to publish a part of his confidential information. Stephenson LJ has given such an example in the course of his judgment.

I therefore agree with Leonard J that it is not an essential ingredient of this defence that the plaintiffs should have been guilty of iniquitous conduct’.

**This case cites:**

- Cited – *Initial Services Ltd -v- Putterill* CA ([1967] 3 All ER 145, [1968] 1 QB 396)  
The plaintiff’s sales manager resigned, but took with him confidential documents which he gave to a newspaper. The defendant sought to justify this, saying that the company had failed to register agreements it should have done under the Act.
- Cited – *Fraser -v- Evans* CA ([1969] 1 QB 349)  
The law of confidence is based on the moral principles of loyalty and fair dealing. An injunction was sought to restrain an intended publication: ‘The court will not restrain the publication of an article, even though it is defamatory, when the . .
- Cited – *Woodward -v- Hutchins* CA ([1977] 2 All ER 751, [1977] 1 WLR 760)  
An injunction was sought to restrain publication of confidential information about a well-known pop group, starring Tom Jones and Engelbert Humperdinck. As the group’s press agent, the defendant’s role had been to see that the group received . .
- Cited – *Hubbard -v- Vosper* CA ([1972] 2 WLR 389, [1971] 1 All ER 1023 CA, [1972] 2 QB 84)  
Claims of infringement were made as to copyright works being various works about Scientology. Extracts had appeared in the defendant’s book which was critical of the cult. It was submitted by the plaintiff that the fair dealing section applied only . .

- Cited – Schering Chemicals Ltd -v- Falkman Ltd CA ([1982] QB 1, [1981] 2 All ER 321, [1981] 2 WLR 848)  
Confidentiality is a relative concept  
Shaw LJ said: ‘ . . the communication in a commercial context of information which at the time is regarded by the giver and recognised by the recipient as confidential and the nature of which has a . .
- Cited – British Steel Corporation -v- Granada Television Ltd HL ([1981] AC 1096, [1981] 1 All ER 452, [1980] 3 WLR 774)  
The defendant had broadcast a TV programme using material confidential to the plaintiff, who now sought disclosure of the identity of the presumed thief.  
Held: (Lord Salmon dissenting) The courts have never recognised a public interest right . .
- Cited – Francome -v- Mirror Group Newspapers Ltd CA ([1984] 1 WLR 892)  
The defendant had acquired illegal tapes of telephone conversations which it said implicated the plaintiff. He sought to restrain publication of the material pending forthcoming disciplinary charges at the Jockey Club.  
Held: The court had to . .
- Cited – Gartside -v- Outram ((1856) 26 LJ Ch113)  
An employee was told by his master ‘I am going to falsify these sales notes and deceive the customers. You are not to say anything about it to anyone.’ He thereafter falsified the sale notes.  
Held: The servant was entitled to say: ‘I am not . .
- Cited – Beloff -v- Pressdram Ltd QBD ([1973] RPC 765, [1973] 1 All ER 241)  
A journalist on The Observer sued the publishers of Private Eye for having published a memorandum of the plaintiff about a politician, Mr Maudling, which had been circulated amongst the employees of The Observer.  
Held: The defences to a claim . .

(This list may be incomplete)

**This case is cited by:**

- Cited – Hyde Park Residence Ltd -v- Yelland, News Group Newspapers Ltd, News International Ltd, Murrell CA (Times 16-Feb-00, Gazette 24-Feb-00, Bailii, [2000] EWCA Civ 37, [2001] Ch 143)  
The court considered a dispute about ownership and confidence in and copyright of video tapes taken by Princess Diana before her death.  
Held: The courts have an inherent discretion to refuse to enforce of copyright. When assessing whether . .
- Considered – Express Newspapers -v- News (UK) plc ([1990] 1 WLR 1320, Times 01-Jan-90, [1990] FSR 359, [1990] Ch D 1320)  
If summary judgment is given to one party on his claim, it must also be given on a counterclaim made on the same basis by the defendant. The principle that a party to litigation cannot ‘approve and reprobate’ (or ‘blow hot and cold’) can curtail a . .
- Approved – Attorney-General -v- Guardian Newspapers Ltd (No 2) (‘Spycatcher’) HL ([1990] 1 AC 109, Bailii, [1988] UKHL 6, [1987] 1 WLR 776, [1988] 3 All ER 545)  
A retired secret service employee sought to publish his memoirs from Australia. The British government sought to restrain publication there, and the defendants sought to report those proceedings, which would involve publication of the allegations . .
- Cited – Mersey Care NHS Trust -v- Ackroyd QBD (Bailii, [2006] EWHC 107 (QB), Times 09-Feb-06)  
The trust, operators of Ashworth Secure Hospital sought from the defendant journalist disclosure of the name of their employee who had revealed to the defendant matters about the holding of Ian Brady, the Moors Murderer, and in particular medical . .
- Cited – McKennitt and others -v- Ash and Another QBD (Bailii, [2005] EWHC 3003 (QB), [2006] EMLR 10)  
The claimant sought to restrain publication by the defendant of a book recounting very personal events in her life. She claimed privacy and a right of confidence. The defendant argued that

there was a public interest in the disclosures.

Held: . .

(This list may be incomplete)

**Last Update:** 14-Apr-16

**Ref:** 223824

<http://swarb.co.uk/lion-laboratories-ltd-v-evans-ca-1985/>

*Caso 2 – Football*



Coletânea da Jurisprudência

CONCLUSÕES DO ADVOGADO-GERAL  
PAOLO MENGOZZI  
apresentadas em 15 de dezembro de 2011<sup>1</sup>

Processo C-604/10

Football Dataco Ltd  
Football Association Premier League Ltd  
Football League Limited  
Scottish Premier League Ltd  
Scottish Football League  
PA Sport UK Ltd  
contra  
Yahoo! UK Limited  
Stan James (Abingdon) Limited  
Stan James PLC  
Enetpulse APS

[pedido de decisão prejudicial apresentado pela Court of Appeal (England & Wales) (Civil Division), Reino Unido]

«Diretiva 96/9/CE — Proteção jurídica das bases de dados — Calendário dos campeonatos de futebol — Direito de autor»

1. No presente processo, o Tribunal de Justiça é chamado a completar a sua própria jurisprudência relativamente à possibilidade de proteger os calendários de um campeonato de futebol com base na Diretiva 96/9/CE, relativa à proteção jurídica das bases de dados (a seguir «Diretiva»)<sup>2</sup>. Em 2004, o Tribunal de Justiça esclareceu que esses calendários não podem, em princípio, gozar da proteção com base no chamado direito «sui generis» previsto pela diretiva. O que se deverá agora verificar, para completar o quadro, é se é aplicável, e em que condições, a proteção fornecida pelo direito de autor.

**I – Quadro jurídico**

2. A Diretiva 96/9/CE prevê que uma base de dados pode beneficiar de dois tipos distintos de proteção. Em primeiro lugar, a proteção assegurada pelo direito de autor definida nos termos seguintes no artigo 3.º:

«1. Nos termos da presente diretiva, as bases de dados que, devido à seleção ou disposição das matérias, constituam uma criação intelectual específica do respetivo autor, serão protegidas nessa qualidade pelo direito de autor. Não serão aplicáveis quaisquer outros critérios para determinar se estas podem beneficiar dessa proteção.

<sup>1</sup> — Língua original: italiano.

<sup>2</sup> — Diretiva 96/9/CE do Parlamento Europeu e do Conselho, de 11 de março de 1996, relativa à proteção jurídica das bases de dados (JO L 77, p. 20).

2. A proteção das bases de dados pelo direito de autor prevista na presente diretiva não abrange o seu conteúdo e em nada prejudica eventuais direitos que subsistam sobre o referido conteúdo».

3. O artigo 7.º da diretiva prevê, assim, um outro tipo de proteção, chamado «sui generis», para as bases de dados cuja elaboração tenha requerido «um investimento substancial»:

«1. Os Estados-Membros instituirão o direito de o fabricante de uma base de dados proibir a extração e/ou a reutilização da totalidade ou de uma parte substancial, avaliada qualitativa ou quantitativamente, do conteúdo desta, quando a obtenção, verificação ou apresentação desse conteúdo representem um investimento substancial do ponto de vista qualitativo ou quantitativo.

[...]

4. O direito previsto no n.º 1 é aplicável independentemente de a base de dados poder ser protegida pelo direito de autor ou por outros direitos. Além disso, esse direito será igualmente aplicável independentemente de o conteúdo da base de dados poder ser protegido pelo direito de autor ou por outros direitos. A proteção das bases de dados pelo direito previsto no n.º 1 não prejudica os direitos existentes sobre o seu conteúdo».

4. O artigo 14.º da diretiva ocupa-se da sua aplicação no tempo. O mesmo indica, em particular, no n.º 2, a regra a aplicar no caso de uma base de dados que estivesse protegida pelo direito de autor antes da entrada em vigor da diretiva, mas não possuísse os requisitos para essa proteção com base na própria diretiva:

«[...] sempre que uma base de dados protegida por um regime de direitos de autor num Estado-Membro à data de publicação da presente diretiva não corresponda aos critérios de elegibilidade para a proteção a título de direito de autor previsto no n.º 1 do artigo 3.º, a presente diretiva não terá por efeito a redução, nesse Estado-Membro, do prazo de proteção concedido a título do regime acima referido ainda por decorrer».

## II – Matéria de facto, processo principal e questões prejudiciais

5. A sociedade Football Dataco Ltd e o. (a seguir «Football Dataco e o.») organizam os campeonatos de futebol ingleses e escoceses. Neste contexto elaboram e tornam público o elenco de todos os encontros que serão jogados, todos os anos, em tais campeonatos. As contrapartes, Yahoo! UK Limited e o. (a seguir «Yahoo e o.») utilizam os calendários de futebol em questão para fornecer notícias e informações e/ou para organizar atividades de apostas.

6. A Football Dataco e o. pedem, em síntese, à Yahoo e o. o pagamento de direitos pela utilização dos calendários de futebol que elaboraram. As mesmas reivindicam para tais calendários a proteção decorrente da diretiva, seja com base no direito de autor seja com base no direito «sui generis».

7. Os juízes nacionais excluíram a proteção com base no direito «sui generis», uma vez que o Tribunal de Justiça já se pronunciou sobre este ponto recentemente e de modo muito claro, em quatro acórdãos proferidos pela Grande Secção em novembro de 2004<sup>3</sup>. Considerando, no entanto, ainda em aberto a problemática relativa à possível proteção com base no direito de autor, que não tinha sido suscitada no âmbito das causas decididas em 2004, o órgão jurisdicional de reenvio suspendeu o processo e colocou as seguintes questões prejudiciais:

«1) No artigo 3.º, n.º 1, da Diretiva 96/9/CE relativa à proteção jurídica das bases de dados, o que se deve entende[r] por 'bases de dados que, devido à seleção ou disposição das matérias, constituam uma criação intelectual específica do respetivo autor' e, em especial,

<sup>3</sup> — Acórdãos de 9 de novembro de 2004, *Pitman Marketing* (C-46/02, Col.ª, p. I-10365); *The British Horseracing Board e o.* (C-203/02, Col.ª, p. I-10415); *Pitman Marketing* (C-338/02, Col.ª, p. I-10497), e *Pitman Marketing* (C-444/02, Col.ª, p. I-10548).

- a) devem o esforço intelectual e a perícia na criação de dados ser excluídos?
  - b) a expressão 'seleção ou [a] disposição' inclui o aditamento de um significado importante a um dado pr[e]existente (como a fixação da data de um jogo de futebol);
  - c) a expressão 'criação intelectual específica do respetivo autor' exige mais do que uma quantidade considerável de trabalho e perícia do autor? Em caso de resposta afirmativa, o quê?
- 2) A diretiva opõe-se à existência de direitos nacionais sob a forma de direitos de autor sobre bases de dados diferentes dos previstos na diretiva?»

### III – Quanto à primeira questão prejudicial:

8. Na sua primeira questão prejudicial o órgão jurisdicional de reenvio pede, em síntese, ao Tribunal de Justiça para precisar em que condições uma base de dados na aceção da Diretiva 96/9/CE pode ser protegida pelo direito de autor. A fim de poder responder de modo adequado é necessário, antes de mais, recapitular a jurisprudência do Tribunal de Justiça relativa aos calendários de futebol, e verificar depois quais são as relações entre os dois tipos de proteção possíveis com base na diretiva: o direito de autor, por um lado, e o direito «sui generis», por outro.

#### A – Jurisprudência do Tribunal de Justiça nesta matéria

9. A jurisprudência do Tribunal de Justiça relativa à proteção das bases de dados, e refiro-me em particular aos já citados acórdãos de novembro de 2004, esclareceu dois pontos fundamentais que devem estar presentes no exame das presentes questões prejudiciais.

10. Em primeiro lugar um calendário de futebol, ainda que constituído por uma simples lista de encontros, deve ser considerado uma base de dados na aceção da diretiva<sup>4</sup>. Tal ponto é dado como assente quer pelo órgão jurisdicional de reenvio quer por todos os interessados que apresentaram observações, e não deve, portanto, ser objeto de análise adicional.

11. Em segundo lugar, um calendário de futebol não satisfaz os requisitos que são necessários, na aceção do artigo 7.º da diretiva, para proteger uma base de dados através do direito «sui generis». Isto na medida em que a redação do calendário, isto é, a inserção de uma lista ordenada de uma série de elementos preexistentes (os dados relativos a cada encontro), não exige qualquer investimento substancial para a obtenção, a verificação ou a apresentação dos dados<sup>5</sup>. Também este aspeto, como indiquei, é dado como assente pelo órgão jurisdicional de reenvio (embora algumas das partes na causa principal tivessem tentado obter que fossem também colocadas ao Tribunal de Justiça algumas questões relativamente ao direito «sui generis»), o qual limitou, portanto, as suas questões à proteção com base no direito de autor.

#### B – Relação entre a proteção baseada no direito de autor e a proteção «sui generis»

12. Um outro ponto, que deve ser necessariamente esclarecido antes de se proceder ao exame da primeira questão, diz respeito à relação entre os dois tipos de proteção previstos pela diretiva. Poder-se-ia de facto perguntar, lendo o texto das disposições aplicáveis, se não existe uma disposição hierárquica entre a proteção com base no direito de autor e a proteção «sui generis». Semelhante

4 — Acórdão no processo *Finarex Marketing* (C-444/02, n.º 23 a 36), já referido na nota 3.

5 — Acórdão no processo *Finarex Marketing* (C-46/02, n.º 46 a 47), já referido na nota 3.

interpretação, que pode contar com o apoio de opiniões abalizadas<sup>6</sup> e também foi invocada indiretamente em algumas observações desenvolvidas na audiência, considera a proteção «sui generis» como uma proteção de segundo nível, que pode ser reconhecida quando uma base de dados não possua a originalidade que é necessária para ser protegida pelo direito de autor. Neste caso, o facto de que o Tribunal de Justiça tenha excluído, nos seus acórdãos de novembro de 2004, a proteção «sui generis» (por assim dizer «menor») para os campeonatos de futebol, implicaria automaticamente excluir também a proteção (por assim dizer «maior») fundada sobre o direito de autor.

13. O exame atento da diretiva mostra, todavia, que semelhante leitura não é correta, e que os dois tipos de proteção devem ser considerados completamente autónomos um do outro, como, de facto, parecem ter aceite, também, todos os interessados que apresentaram observações no presente processo, incluindo-se aí a Comissão.

14. Deve, com efeito, observar-se que, na diretiva, o próprio objeto das duas proteções é distinto. Por um lado, a proteção baseada no direito de autor concentra-se essencialmente na *estrutura* da base de dados, isto é, no modo como esta foi concretamente criada pelo seu autor, através da escolha dos materiais a incluir ou as modalidades da sua apresentação. O n.º 2 do artigo 3.º precisa, de resto, claramente que o direito de autor previsto em tal artigo «não abrange o [...] conteúdo» da base de dados, que pode ser protegido pelo direito de autor de forma autónoma, mas não o é devido ao facto de estar inserido numa base de dados protegida. O décimo quinto considerando observa que a proteção do direito de autor «incide sobre a estrutura da base». Pelo contrário, a proteção «sui generis» é simplesmente um direito de proibir operações de extração e/ou de reutilização *nos dados contidos nas bases de dados*. Este direito é reconhecido para proteger não a originalidade da base de dados em si, mas para compensar o esforço desenvolvido para reunir, verificar e/ou apresentar os dados contidos na mesma<sup>7</sup>.

15. Por outros termos, uma base de dados pode, portanto, conforme os casos, ser protegida apenas pelo direito de autor, apenas pelo direito «sui generis», por ambos ou, também, por nenhum dos dois.

#### C — Noção de base de dados na aceção da diretiva

16. O facto de, como acabámos de ver, os dois tipos de proteção possíveis da base de dados serem de todo independentes um do outro, não significa todavia que a noção de base de dados, tal como foi desenvolvida pelo Tribunal de Justiça nos seus acórdãos de novembro de 2004, deva ser diferente em relação aos dois tipos de direito. Pelo contrário, é minha convicção que tal noção deve ser necessariamente idêntica. Não faz qualquer sentido que um conceito chave da diretiva, definido no seu artigo 1.º possa ter um alcance diferente, sem algum argumento textual nesse sentido, para interpretar dois artigos distintos do texto normativo, que conservam de resto todo o seu valor interpretados à luz de uma noção unitária do conceito de base de dados. O direito de autor pode proteger a estrutura da base de dados, enquanto o direito «sui generis» protege o conteúdo: mas isto não exige de modo algum que existam duas noções diferentes de «base de dados».

17. Neste contexto, o Tribunal de Justiça clarificou que o âmbito de proteção oferecido pela diretiva *não compreende a fase da criação dos dados, mas apenas a fase da recolha, verificação e apresentação*

6 — Neste sentido v., em particular, o *working paper* da DG Mercado Interno 12 de dezembro de 2005, *First evaluation of Directive 96/9/EC on the legal protection of databases*, disponível no sítio Web da Comissão.

7 — Acórdão no processo *Fituram Marketing* (C-46/02, n.º 39), já referido na nota 3. Deve notar-se incidentalmente que a versão italiana do artigo 7.º da diretiva parece exigir que se tenha verificado um investimento substancial na obtenção, na verificação e na apresentação dos dados. Em contrapartida, as outras versões linguísticas utilizam a conjunção ou, e com isto é coerente a interpretação fornecida pelo Tribunal de Justiça: o investimento substancial pode ocorrer também se diz respeito apenas à obtenção, apenas à verificação ou apenas à apresentação dos dados.

*dos mesmos*<sup>8</sup>. Por outras palavras, o intérprete deve individualizar a «base de dados», tendo a atenção de traçar com clareza uma linha que distinga o momento da criação dos dados, que não interessa à diretiva, do momento em que tais dados são recolhidos ou elaborados, o qual por sua vez releva para determinar se tal base de dados merece pelo menos uma proteção.

18. O Tribunal de Justiça efetuou esta distinção, entre criação dos dados e a sua inserção, no âmbito de um discurso sobre a proteção «sui generis». Em meu entender, todavia, trata-se de considerações que dizem respeito, de modo mais geral, à própria noção de base de dados na aceção da diretiva. Essa precisão esclarece além disso de modo definitivo que a diretiva protege a *criação de bases de dados* — sobre os dois perfis da estrutura desses e da recolha dos dados — *mas não se ocupa da proteção dos dados enquanto tais*. De resto, o objetivo da diretiva é o de favorecer a criação dos sistemas de recolha e consulta de informações<sup>9</sup>, não a criação dos dados. Na sua discussão relativa à noção de base de dados o Tribunal de Justiça insistiu, por outro lado, repetidamente sobre o valor informativo independente dos dados inseridos na base<sup>10</sup>.

19. O facto de se deixar de tomar em consideração, para efeitos da diretiva, a atividade de criação dos dados, é, de resto, perfeitamente lógico, também, com referência ao direito de autor, a partir do momento em que, como sublinha a diretiva, os dados *podem de qualquer modo ser protegidos, enquanto tais, pelo direito de autor*, se se verificarem os requisitos para tanto, independentemente da existência de um direito de autor sobre a base de dados.

20. Devo por outro lado observar que, no caso presente, a própria ideia de utilizar a proteção do direito de autor para proteger os calendários de futebol parece pelo menos singular. Como já salientei antes, de facto o direito de autor protege essencialmente, no caso de uma base de dados, a parte «exterior», da sua estrutura. Tanto quanto se pode compreender, a Yahoo utiliza os *dados* elaborados pelas sociedades organizadoras dos campeonatos, e não as eventuais modalidades em que essas sociedades tornam os dados públicos. Muito razoavelmente, antes que os acórdãos do Tribunal de Justiça de 2004 excluíssem a sua aplicabilidade, o único tipo de proteção considerado pelas sociedades organizadoras era a proteção «sui generis», que tutela, como se viu, mais o conteúdo de uma base de dados (ou, melhor dizendo, o esforço necessário para os recolher e apresentar) do que a sua estrutura. A utilização do direito de autor aparece aqui como uma solução de recurso, resultante da exclusão da proteção «sui generis» por parte do Tribunal de Justiça. Por outro lado, não é de modo nenhum certo que a eventual existência de uma proteção baseada sobre o direito de autor para os calendários de futebol impedisse a atividade atualmente desenvolvida pela Yahoo, que, tanto quanto nos é dado compreender das peças do processo, parece limitar-se ao uso dos dados em bruto (datas, horários e equipas dos vários encontros), e não da estrutura da base de dados.

21. Tudo isto ponderado, é agora possível passar ao exame das três subquestões colocadas pelo órgão jurisdicional de reenvio. A apreciação destas permitirá, como veremos, apresentar uma resposta de conjunto à primeira questão prejudicial.

#### D — Quanto à primeira questão prejudicial, alínea a)

22. Na primeira das três subquestões o órgão jurisdicional de reenvio pergunta ao Tribunal de Justiça se a atividade desenvolvida para a criação dos dados que são inseridos na base de dados deve ser tomada em consideração para determinar se essa base de dados merece, pelo menos, a proteção com base no direito de autor.

8 — Acórdão no processo *Fiturax Marketing* (C-444/02, n.º 39 a 40), já referido na nota 3, e no processo *Fiturax Marketing* (C-535/02, n.º 25), já referido na nota 3.

9 — Acórdão no processo *Fiturax Marketing* (C-444/02, n.º 38), já referido na nota 3.

10 — *Ibidem*, n.º 29 e 33 a 35.

23. A resposta a esta interrogação deriva diretamente de quanto observei antes, no que respeita à noção necessariamente unitária de «base de dados» da diretiva. Os esforços desenvolvidos para a criação dos dados não podem entrar em linha de conta para avaliar o direito à proteção com base no direito de autor, exatamente como esses não podem entrar em linha de conta, segundo o ensinamento do Tribunal de Justiça, para avaliar o direito à proteção «sui generis». A criação dos dados é uma atividade que se coloca fora do campo de aplicação da diretiva.

24. De resto, já se observou que a atividade desenvolvida para a criação dos dados não pode ser, como o Tribunal de Justiça afirmou, tomada em consideração para a proteção «sui generis», que é aquela mais estreitamente ligada aos dados e à sua obtenção, por maioria de razão tais atividades deverão ser ignoradas no que respeita à proteção mediante o direito de autor, a qual apresenta uma ligação mais ténue com a recolha dos dados e é, antes, focalizada na sua apresentação.

E – Quanto à primeira questão prejudicial, alínea b)

25. Na segunda subquestão, o órgão jurisdicional de reenvio pede ao Tribunal de Justiça que esclareça se a «seleção ou a disposição» dos conteúdos da base de dados, cujo exame permite verificar se existem os pressupostos para a proteção segundo o direito de autor, podem consistir, também, num aumento de importância relevante de dados preexistentes.

26. Em síntese, aquilo que se pergunta é se constitui uma operação de «seleção ou [...] disposição» suficiente para garantir a proteção com base no artigo 3.º o facto de, por exemplo, se atribuir características específicas posteriores a um elemento inserido na base de dados. O órgão jurisdicional de reenvio menciona, a título de exemplo, o facto de se fixar a data de um determinado encontro entre duas equipas de futebol.

27. Considero que a subquestão agora indicada parte de um pressuposto errado. De facto, todas as indicações referentes a cada jogo de um determinado campeonato *devem considerar-se definidas antes da introdução dos dados na base de dados*. Conforme o Tribunal de Justiça já esclareceu, no caso de um calendário de futebol, os dados de partida que são inseridos na base de dados não são todas as equipas e todas as datas possíveis, *mas as circunstâncias específicas de todos e cada um dos encontros que deverá ser disputado* (data, equipa, lugar, etc.)<sup>11</sup>. Por outras palavras, a determinação de todas as características de todos os encontros coloca-se na fase da criação dos dados — excluída, como se viu, da proteção com base na diretiva — e não pode ser considerada como um resultado ou uma consequência da organização dos dados na base de dados.

28. O órgão jurisdicional de reenvio, no entanto, parece partir do pressuposto de que, na base de dados, estão inseridas, na prática, algumas listas simples: todas as equipas do campeonato, todas as datas e todos os horários possíveis para os encontros. Deste ponto de vista, a determinação das características específicas de cada encontro (equipas envolvidas, dia e hora) ocorreria *depois* da introdução dos dados de partida na base de dados. Tal determinação seria um *produto* da base de dados.

29. Em meu entender, semelhante interpretação dos factos é errada. O que se insere na base de dados não são as composições genéricas das equipas, das datas e dos horários possíveis. O que se insere na base de dados são já, pelo contrário, todos os encontros individualizados que deverão ser disputados, *cada um com as suas características completas*: hora, data, equipas. A passagem da lista genérica (por exemplo a equipa A, B, C, D, etc., as datas x, y, z, etc.) à definição dos encontros específicos (por exemplo, equipa A contra a equipa B na data x) *coloca-se na fase da criação dos dados*, anterior à inserção destes na base de dados.

11 — Acórdão no processo *Pitman Marketing* (C-46/02, n.º 41 e 42), já referido na nota 3; no processo *Pitman Marketing* (C-338/02, n.º 31), já referido na nota 3, e no processo *Pitman Marketing* (C-444/02, n.º 47), já referido na nota 3.

30. Por consequência, são irrelevantes as observações, bastante detalhadas, desenvolvidas pelas partes recorrentes no processo principal para demonstrar que o trabalho de determinação das características de cada partida individual não é puramente automático e exige, pelo contrário, considerável perícia e competência. Esta atividade é, de facto, em todos os aspetos preliminar e distinta em relação à da criação da base de dados.

31. A interpretação que acabo de referir é confirmada pela própria jurisprudência do Tribunal de Justiça, em particular nas passagens em que é sublinhada a necessidade de que os componentes específicos de uma base de dados possuam um valor informativo autónomo<sup>12</sup>. Não podem, de facto, ser consideradas como autenticamente «informativas», em meu entender, listas genéricas de equipas, datas e horários. Apenas o conjunto das características de cada um dos encontros individuais pode ter semelhante valor.

32. Dito isto, considero que a subquestão, quando posta em termos abstratos e fora das circunstâncias do presente processo, deveria receber uma resposta positiva. Por outros termos, a atribuição de uma relevância significativa a elementos dos dados preexistentes — realizada mediante a inserção de tais dados numa base de dados — pode representar uma «disposição das matérias» merecedora de ser considerada para efeitos da proteção com base no direito de autor. Não existem de facto, em meu entender, dúvidas que no espírito da diretiva, o facto de que a inserção dos dados numa base de dados acrescenta aos mesmos um valor adicional ou significado que pode ser relevante, no âmbito de uma avaliação de conjunto, para reconhecer a proteção do direito de autor à própria base de dados. Isto é, de resto, precisamente o objetivo da disposição, que visa proteger aquilo que uma base de dados «acrescenta», de qualquer modo, em relação aos dados de partida que são inseridos na mesma. No entanto, no caso dos elementos que caracterizam os encontros de um campeonato de futebol, todos eles são parte dos dados de partida, e não um produto da inserção destes últimos na base de dados.

*F – Quanto à primeira questão prejudicial, alínea c)*

33. Na terceira subquestão, o órgão jurisdicional de reenvio interroga o Tribunal de Justiça sobre a noção de «criação intelectual» do autor de uma base de dados. Isto está, evidentemente, em relação com o facto de o artigo 3.º da diretiva subordinar a proteção com base no direito de autor precisamente ao facto de a base de dados, devido à seleção ou disposição das matérias, constituir uma criação intelectual específica do respetivo autor. Em particular, o órgão jurisdicional de reenvio pergunta se, para haver uma criação intelectual, é suficiente, pelo menos, uma contribuição significativa de trabalho e perícia («significant labour and skill»).

34. Também esta terceira subquestão, com toda a probabilidade, parte como a precedente da premissa, em meu entender errada, de que os esforços desenvolvidos pelas sociedades organizadoras para determinar as equipas, as datas e os horários dos vários encontros do campeonato, esforços que, indubitavelmente, exigem uma determinada quantidade de trabalho e de experiência organizativa, estariam ligados à realização da base de dados. Na realidade, como salientei acima, esses esforços devem, pelo contrário, ser colocados na fase precedente, a da criação dos dados, a qual não pode ser tomada em consideração para avaliar o direito da proteção da base de dados.

35. Em qualquer caso, ainda que abandonando essas considerações e examinando o pedido do órgão jurisdicional nacional em termos abstratos, a resposta é, em meu entender, obrigatória: a proteção do direito de autor está subordinada ao facto de a base de dados ser caracterizada por um elemento «criador», e não é suficiente que a criação da base de dados tenha exigido trabalho e perícia.

<sup>12</sup> — V., *supra*, nota 10.

36. É sabido que, no interior da União, existem parâmetros diferentes no que respeita ao nível de originalidade exigido, em geral, para reconhecer a proteção do direito de autor<sup>13</sup>. Em particular, em alguns países da União, os que se caracterizam por uma tradição de *common law*, o critério de referência é tradicionalmente o contributo de «trabalho, perícia ou esforço» (labour skills or effort). Por exemplo, no Reino Unido, por esta razão, as bases de dados gozavam, em geral, antes da entrada em vigor da diretiva, da proteção do direito de autor. Uma base de dados era protegida pelo direito de autor se o seu criador tinha necessitado, para a realizar, de efetuar um esforço ou utilizar uma certa perícia. Pelo contrário, nos países de tradição continental é, em geral, exigido, para reconhecer uma proteção com base no direito de autor, que a obra possua um elemento de criatividade, ou exprima, de qualquer modo, a personalidade do seu autor, embora esteja sempre excluída qualquer apreciação relativa à qualidade ou à natureza «artística» da obra.

37. Ora, a este propósito não existem dúvidas quanto ao facto de que a diretiva acolheu, no que respeita à proteção com base no direito de autor, uma noção de originalidade que vai para além do simples esforço «mecânico» necessário para recolher os dados e inseri-los na base. Para estar protegida pelo direito de autor, a base de dados deve, como indica explicitamente o artigo 3.º da diretiva, ser uma «criação intelectual» do seu autor. Tal expressão não deixa lugar a dúvidas e retoma uma fórmula típica da tradição continental do direito de autor.

38. É claro que não é possível definir de uma vez por todas, em termos gerais, quando se está em presença de uma «criação intelectual». Trata-se de uma avaliação que, como referi, não é necessária no caso presente. De qualquer modo, quando essa avaliação se impuser, a mesma compete ao juiz nacional, com base nas circunstâncias de cada caso concreto.

39. O Tribunal de Justiça teve ocasião de fornecer a este propósito algumas indicações e, em particular, sublinhou que a proteção do direito de autor, reconhecida pelo artigo 3.º da diretiva, às bases de dados, bem como pelo artigo 1.º, n.º 3, da Diretiva 91/250<sup>14</sup> aos programas para computador e pelo artigo 6.º da Diretiva 2006/116<sup>15</sup> às fotografias, pressupõe que se trate de obras «originais, na aceção de que são criação intelectual do próprio autor»<sup>16</sup>.

40. A este propósito, o Tribunal de Justiça também teve oportunidade de indicar que se está em presença de uma criação intelectual do autor quando a obra reflete a sua personalidade, isto é, se verifica que o autor pôde efetuar, a esse propósito, escolhas livres e criativas<sup>17</sup>. Além disso, especificou que, em geral, não se está em presença da necessária originalidade quando as características de uma obra são impostas pela função técnica desta última<sup>18</sup>.

41. O que o legislador da diretiva procurou realizar, em síntese, é uma espécie de compromisso/conciliação das orientações existentes nos vários Estados da União na data da aprovação da diretiva. Para a proteção segundo o direito de autor foi escolhido o paradigma mais «rigoroso» dos países de tradição continental, enquanto para a proteção «sui generis» foi utilizado um critério de referência que é mais próximo, na prática, daquele da tradição de *common law*<sup>19</sup>.

13 — Já na proposta inicial da diretiva da Comissão, datada de 13 de maio de 1992 [COM (92) 24 final], as divergências nacionais relativamente à originalidade eram indicadas em três pontos que militavam para uma harmonização da proteção das bases de dados (v. ponto 2.2.5).

14 — Diretiva 91/250/CEE do Conselho, de 14 de maio de 1991, relativa à proteção jurídica dos programas para computador (JO L 122, p. 42).

15 — Diretiva 2006/116/CE do Parlamento Europeu e do Conselho, de 12 de dezembro de 2006, relativa à duração da proteção do direito de autor e de alguns direitos conexos (versão codificada) (JO L 372, p. 12).

16 — Acórdão de 16 de julho de 2009, Infopaq Internacional (C-5/08, Col.ª, p. 1-6569, n.º 35). Deve-se, no entanto, observar que as três diretivas agora citadas utilizam uma terminologia que, em algumas línguas, é idêntica, enquanto noutras (como, por exemplo, no italiano), embora apresentando ligadas diferenças, mostra claramente a intenção do legislador de se referir à mesma noção.

17 — Acórdão de 1 de dezembro de 2011, Patzer (C-143/10, Col.ª, p. 1-12583, n.º 88-89).

18 — Acórdão de 22 de dezembro de 2010, *Espececentri softwarevi auctore* (C-393/09, Col.ª, p. 1-13971, n.º 46).

19 — V., sobre este ponto, também o Working Paper da Comissão, já referido na nota 6 (ponto 1.1).

42. Trata-se, como se vê, de indicações sobretudo gerais, que no entanto não é necessário aqui aprofundar ulteriormente uma vez que, como indiquei antes, no caso de um calendário de futebol confluem na base de dados informações autónomas e já completas *que não adquirem qualquer significado adicional através da sua inserção na própria base de dados.*

43. O facto de a proteção do direito de autor para as bases de dados estar sujeita a um requisito de originalidade mais exigente não significa, naturalmente, que os esforços «mecânicos» para a recolha dos dados sejam irrelevantes para efeitos da diretiva. Pelo contrário, o escopo essencial do seu artigo 7.º, relativo à proteção «sui generis», é precisamente o de proteger tais atividades. O facto de o Tribunal de Justiça de Justiça ter excluído a aplicação, no caso dos calendários de futebol, não lhes reduz a importância em termos mais gerais.

44. Resta, no entanto, o facto de, em princípio, também um calendário de futebol poder, em algumas condições, ser protegido pelo direito de autor, se na sua realização prática o autor introduz elementos com suficiente originalidade. Por exemplo, um calendário caracterizado por uma particular modalidade de representação dos encontros, com a utilização de cores e outros elementos gráficos, poderia, sem dúvida, merecer a proteção do direito de autor com base na diretiva. Esta proteção, todavia, limitar-se-ia a cobrir a *modalidade* da representação, e não os dados nela contidos. Não se verifica que, no caso em exame, o calendário de futebol produzido pelas sociedades organizadoras dos campeonatos se caracterize por uma, seja qual for, modalidade original de apresentação dos dados: compete todavia ao juiz nacional verificar essa circunstância, tendo para esse fim também em conta as suprarreferidas indicações fornecidas pelo Tribunal de Justiça.

#### *G – Conclusão sobre a primeira questão prejudicial*

45. O exame das três subquestões permitiu esclarecer alguns aspetos essenciais da proteção das bases de dados pelo direito de autor, com base na diretiva. Esclareceu-se, em particular, que o esforço desenvolvido para a criação dos dados não pode ser tomado em consideração para avaliar o direito à proteção da base de dados enquanto tal (primeira subquestão). Em segundo lugar, viu-se que embora o acrescento de novos elementos aos dados pré-existentes, como consequência da sua inserção na base de dados, possa ser significativo para avaliar se existe direito à proteção, no caso de uma série de encontros de futebol inseridos numa base de dados não se verifica «enriquecimento» algum dos dados pré-existentes (segunda subquestão). Verificou-se, finalmente, que o simples desenvolvimento de esforços ou perícia não basta para fazer que uma base de dados constitua uma criação intelectual protegida pelo direito de autor (terceira subquestão). Com base nestas observações, é agora possível formular uma resposta à primeira questão prejudicial.

46. Proponho, pois, ao Tribunal de Justiça que decida a primeira questão prejudicial declarando que uma base de dados pode ser protegida pelo direito de autor, na aceção do artigo 3.º da Diretiva 96/9/CE, apenas quando a mesma constitua uma criação intelectual original do respetivo autor. Para esse efeito, não podem ser tomadas em consideração as atividades desenvolvidas para a criação dos dados. No caso de um calendário de futebol, constitui atividade de criação dos dados a determinação de todos os elementos relativos a cada encontro individual.

#### **IV – Quanto à segunda questão prejudicial**

47. Na segunda questão prejudicial, o órgão jurisdicional de reenvio pede ao Tribunal de Justiça que indique se a proteção com base no direito de autor, referida na diretiva, é a única deste tipo possível para uma base de dados ou se, no entanto, o direito nacional, pelo contrário, pode reconhecer a mesma proteção também às bases de dados que, na aceção da diretiva, não possuem os necessários requisitos.

48. O mesmo órgão jurisdicional nacional indica claramente, no seu despacho, ter apenas dúvidas bastante ténues sobre a resposta à questão, e, com efeito, a mesma presta-se a ser decidida rapidamente. É evidente, de facto, que a diretiva realizou, em matéria de proteção das bases de dados pelo direito de autor, uma harmonização exaustiva que não admite direitos adicionais reconhecidos a nível nacional.

49. Desde logo, a leitura dos considerandos da diretiva mostra, sem ambiguidade, que tal é a vontade do legislador. Por exemplo, no terceiro considerando observa-se o seguinte:

«Considerando que é necessário eliminar as diferenças existentes que têm um efeito de distorção no funcionamento de mercado interno e evitar que surjam novas diferenças, ao passo que as diferenças que presentemente não afetam negativamente o funcionamento do mercado interno ou o desenvolvimento de um mercado da informação na Comunidade podem não ser suprimidas ou impedidas».

50. O décimo segundo considerando alinha na mesma ordem de ideias:

«Considerando que um investimento desta natureza em sistemas modernos de armazenamento e tratamento da informação não poderá ser realizado na Comunidade sem um regime jurídico estável e homogêneo de proteção dos direitos de fabricantes das bases de dados».

51. O argumento que encerra definitivamente a questão é, no entanto, em meu entender, o artigo 14.<sup>o</sup> da diretiva. Essa norma prevê um regime transitório especial para as bases de dados que, anteriormente protegidas pelo direito de autor com base nas normas nacionais, não satisfazem os requisitos para a proteção com base no direito de autor na aceção da diretiva. Essas bases de dados conservam, para o restante período de proteção concedido com base no regime nacional anterior à diretiva, a proteção do direito de autor. É evidente que a norma não teria qualquer sentido se, depois da entrada em vigor da diretiva, um direito nacional pudesse continuar a reconhecer, sem limite de tempo, a proteção a uma base de dados que não possuísse os requisitos na aceção da diretiva. Se assim fosse, de facto, o direito de autor «nacional» continuaria a ser aplicável de forma autónoma e não haveria necessidade alguma de prever uma norma transitória para as bases de dados que, na aceção da diretiva, não são suficientemente originais para merecer essa proteção.

52. A segunda questão prejudicial deve, portanto, ser decidida declarando que a diretiva se opõe a que um direito nacional reconheça a proteção do direito de autor a uma base de dados que não possui os requisitos indicados no artigo 3.<sup>o</sup> dessa diretiva.

## V – Conclusões

53. Com base nas considerações antes desenvolvidas, proponho ao Tribunal de Justiça que responda nos termos seguintes às questões prejudiciais colocadas pela Court of Appeal:

- «1. Uma base de dados pode ser protegida pelo direito de autor, na aceção do artigo 3.<sup>o</sup> da Diretiva 96/9/CE, apenas quando a mesma constitua uma criação intelectual original do respetivo autor. Para esse efeito, não podem ser tomadas em consideração as atividades desenvolvidas para a criação dos dados. No caso de um calendário de futebol, constitui atividade de criação dos dados a determinação de todos os elementos relativos a cada encontro individual.
2. A referida diretiva opõe-se a que um direito nacional reconheça a proteção do direito de autor a uma base de dados que não possui os requisitos indicados no artigo 3.<sup>o</sup> dessa diretiva».

*Caso 3 - Ryanair*



Coletânea da Jurisprudência

ACÓRDÃO DO TRIBUNAL DE JUSTIÇA (Segunda Secção)

15 de janeiro de 2015\*

«Reenvio prejudicial — Diretiva 96/9/CE — Proteção jurídica das bases de dados — Base de dados que não está protegida pelo direito de autor nem pelo direito sui generis — Limitação contratual dos direitos dos utilizadores da base de dados»

No processo C-30/14,

que tem por objeto um pedido de decisão prejudicial apresentado, nos termos do artigo 267.º TFUE, pelo Hoge Raad der Nederlanden (Países Baixos), por decisão de 17 de janeiro de 2014, que deu entrada no Tribunal de Justiça em 22 de janeiro de 2014, no processo

**Ryanair Ltd**

contra

**PR Aviation BV,**

O TRIBUNAL DE JUSTIÇA (Segunda Secção),

composto por: R. Silva de Lapuerta, presidente de secção, K. Lenaerts (relator), vice-presidente do Tribunal de Justiça, J.-C. Bonichot, A. Arabadjiev e J. L. da Cruz Vilaça, juizes,

advogado-geral: Y. Bot,

secretário: C. Strömholm,

vistos os autos e após a audiência de 12 de novembro de 2014,

vistas as observações apresentadas:

- em representação da Ryanair Ltd, inicialmente, por M. van Heezik, A. van Aerde e R. Le Poole e, em seguida, por A. van Aerde e R. Le Poole, advocaten,
  - em representação da PR Aviation BV, por A. Groen, advocaat,
  - em representação da Comissão Europeia, por J. Samnadda e F. Wilman, na qualidade de agentes,
- vista a decisão tomada, ouvido o advogado-geral, de julgar a causa sem apresentação de conclusões, profere o presente

\* Língua do processo: neerlandês.

**Acórdão**

- 1 O pedido de decisão prejudicial tem por objeto a interpretação da Diretiva 96/9/CE do Parlamento Europeu e do Conselho, de 11 de março de 1996, relativa à proteção jurídica das bases de dados (JO L 77, p. 20).
- 2 Este pedido foi apresentado no âmbito de um litígio que opõe a Ryanair Ltd (a seguir «Ryanair») à PR Aviation BV (a seguir «PR Aviation»), a respeito da utilização, por esta última, de dados provenientes do sítio Internet da Ryanair.

**Quadro jurídico***Direito da União*

- 3 A Diretiva 96/9 tem quatro capítulos.
- 4 No capítulo I da Diretiva 96/9, intitulado «Âmbito de aplicação», o seu artigo 1.º, sob a mesma epígrafe, dispõe, nos seus n.ºs 1 e 2:

«1. A presente diretiva diz respeito à proteção jurídica das bases de dados, seja qual for a forma de que estas se revistam.

2. Para efeitos da presente diretiva, entende-se por 'base de dados', uma coletânea de obras, dados ou outros elementos independentes, dispostos de modo sistemático ou metódico e suscetíveis de acesso individual por meios eletrónicos ou outros.»

- 5 No capítulo II da diretiva, intitulado «Direito de autor», figura o artigo 3.º, sob a epígrafe «Objeto da proteção», cujo n.º 1 prevê:

«Nos termos da presente diretiva, as bases de dados que, devido à seleção ou disposição das matérias, constituam uma criação intelectual específica do respetivo autor, serão protegidas nessa qualidade pelo direito de autor. Não serão aplicáveis quaisquer outros critérios para determinar se estas podem beneficiar dessa proteção.»

- 6 No capítulo II, o artigo 5.º da referida diretiva, sob a epígrafe «Atos sujeitos a restrições», tem a seguinte redação:

«O autor de uma base de dados beneficia do direito exclusivo de efetuar ou autorizar os seguintes atos relativos à forma de expressão protegida pelo direito de autor:

- a) Reprodução permanente ou provisória, total ou parcial, por quaisquer meios e sob qualquer forma;
- b) Tradução, adaptação, transformação ou qualquer outra modificação;
- c) Qualquer forma de distribuição da base ou de uma cópia ao público. [...]
- d) Qualquer comunicação, exposição ou representação pública;
- e) Qualquer reprodução, distribuição, comunicação, exposição ou representação pública dos resultados dos atos citados na alínea b).»

- 7 No mesmo capítulo II, o artigo 6.º, n.º 1, da mesma diretiva, sob a epígrafe «Exceções aos atos sujeitos a restrições», dispõe:

«O utilizador legítimo de uma base de dados ou das suas cópias pode efetuar todos os atos enumerados no artigo 5.º, necessários para aceder ao conteúdo da base de dados e para a utilizar em condições normais sem autorização do autor da base. Se o utilizador legítimo estiver autorizado a utilizar apenas uma parte da base de dados, o presente número é aplicável unicamente a essa parte.»

- 8 No capítulo III da Diretiva 96/9, intitulado «Direito *sui generis*», figura o artigo 7.º, sob a epígrafe «Objeto da proteção», que dispõe, nos seus n.ºs 1 e 5:

«1. Os Estados-Membros instituirão o direito de o fabricante de uma base de dados proibir a extração e/ou a reutilização da totalidade ou de uma parte substancial, avaliada qualitativa ou quantitativamente, do conteúdo desta, quando a obtenção, verificação ou apresentação desse conteúdo representem um investimento substancial do ponto de vista qualitativo ou quantitativo.

[...]

5. Não serão permitidas a extração e/ou reutilização [repetidas] e sistemáticas de partes não substanciais do conteúdo da base de dados que pressuponham atos contrários à exploração normal dessa base, ou que possam causar um prejuízo injustificado aos legítimos interesses do fabricante da base.»

- 9 No mesmo capítulo III figura o artigo 8.º da mesma diretiva, sob a epígrafe «Direitos e obrigações do utilizador legítimo», que dispõe:

«1. O fabricante de uma base de dados posta à disposição do público, seja por que meio for, não pode impedir o utilizador legítimo dessa base de extrair e/ou reutilizar partes não substanciais do respetivo conteúdo, avaliadas qualitativa ou quantitativamente, para qualquer efeito. Se o utilizador legítimo estiver autorizado a extrair e/ou a reutilizar apenas uma parte da base de dados, o presente número é aplicável unicamente a essa parte.

2. O utilizador legítimo de uma base de dados posta à disposição do público, seja por que meio for, não pode praticar quaisquer atos que colidam com a exploração normal dessa base, ou lesem injustificadamente os legítimos interesses do fabricante da base.

3. O utilizador legítimo de uma base de dados posta à disposição do público, seja por que meio for, não pode prejudicar o titular de um direito de autor ou de um direito conexo sobre obras ou prestações contidas nessa base.»

- 10 No capítulo IV da Diretiva 96/9, intitulado «Disposições comuns», o artigo 15.º, sob a epígrafe «Caráter imperativo de certas disposições», enuncia:

«É nula qualquer disposição contratual contrária ao n.º 1 do artigo 6.º e ao artigo 8.º.»

#### *Direito neerlandês*

- 11 A Diretiva 96/9 foi transposta para o direito neerlandês pela Lei de adaptação da legislação neerlandesa à Diretiva 96/9/CE, do Parlamento Europeu e do Conselho, de 11 de março de 1996, relativa à proteção jurídica das bases de dados (Wet houdende aanpassing van de Nederlandse wetgeving aan richtlijn 96/9/EG van het Europees Parlement en de Raad van 11 maart 1996 betreffende de rechtsbescherming van databanken), de 8 de julho de 1999 (Stb. 1999, p. 303; a seguir «lei sobre as bases de dados»).

12 A Lei dos direitos de autor (Auteurswet, a seguir «Aw») dispõe, no seu artigo 1.º:

«O direito de autor é o direito exclusivo do autor de uma obra literária, científica ou artística, ou dos seus sucessores, de a divulgar e reproduzir, sob reserva das limitações previstas pela lei.»

13 O artigo 10.º da Aw dispõe:

«1. Para efeitos da presente lei, entende-se por obra literária, científica ou artística:

1º os livros, folhetos, jornais, revistas e todos os outros escritos;

[...]

3. As coletâneas de obras, de dados ou de outros elementos independentes, dispostos de modo sistemático ou metódico e individualmente acessíveis por meios eletrónicos ou por outra forma, são, sem prejuízo de outros direitos sobre a coletânea e sem prejuízo do direito de autor ou de outros direitos sobre as obras, dados ou outros elementos contidos na coletânea, protegidos como obras independentes.

[...]

14 Nos termos do artigo 24.ª da Aw:

«1. Não é considerada uma infração do direito de autor sobre uma coletânea, na aceção do artigo 10.º, n.º 3, a reprodução feita pelo utilizador legítimo da coletânea, que é necessária para obter o acesso à coletânea de dados e fazer uma utilização normal.

[...]

3. Os n.ºs 1 e 2 não podem ser derogados por contrato em prejuízo do utilizador legítimo.»

#### Litígio no processo principal e questão prejudicial

15 A PR Aviation explora um sítio Internet onde os consumidores podem fazer buscas nos dados de voo das companhias aéreas de baixo custo, comparar os preços e, mediante o pagamento de uma comissão, reservar um voo. A PR Aviation obtém os dados necessários para responder a uma busca individual, por via automatizada, designadamente, a partir de uma coletânea de dados ligada ao sítio Internet da Ryanair, igualmente acessível aos consumidores.

16 O acesso ao referido sítio Internet pressupõe que o visitante aceita a aplicação das condições gerais da Ryanair, preenchendo uma quadrícula para esse efeito. Na data dos factos do processo principal, essas condições continham as seguintes cláusulas:

«2. Distribuição exclusiva. Este sítio Internet e o centro de chamadas telefónicas da Ryanair são os distribuidores exclusivos dos serviços da Ryanair. A Ryanair.com é o único sítio Internet autorizado a vender voos da Ryanair. A Ryanair não autoriza outros sítios a vender os seus voos, quer para reservas de voos simples quer para reservas fixas e estadas (package). [...]

3. Utilizações permitidas. A utilização deste sítio Internet só é permitida para os seguintes fins privados e não comerciais: (i) consultar este sítio Internet; (ii) efetuar reservas; (iii) verificar/alterar reservas; (iv) consultar informações sobre chegadas/partidas; (v) efetuar check-in em linha; (vi) consultar outros sítios Internet através de ligações fornecidas neste sítio Internet; (vii) utilizar outras funcionalidades eventualmente disponibilizadas neste sítio Internet.

É proibida a utilização de sistemas automatizados ou de *software* para extrair dados desse sítio Internet ou do sítio Internet [www.bookryanair.com](http://www.bookryanair.com), para fins comerciais (captura de dados no ecrã) ('screen scraping'), exceto se os terceiros tiverem celebrado um contrato de licença por escrito com a Ryanair, nos termos do qual é autorizado o acesso à parte em questão, unicamente com o objetivo de comparação de preços, às informações da Ryanair sobre os preços, voos e horários.»

- 17 Invocando a Diretiva 96/9, a lei sobre as bases de dados e a Aw, a Ryanair alega que a PR Aviation violou os seus direitos sobre a sua coletânea de dados e agiu sem observar as condições gerais de utilização do seu sítio Internet, contudo aceites pela PR Aviation. A Ryanair pediu que a PR Aviation fosse condenada a abster-se de qualquer infração aos seus direitos, sob pena do pagamento de uma sanção pecuniária compulsória, bem como de lhe pagar uma indemnização.
- 18 Por sentença de 28 de julho de 2010, o Rechtbank Utrecht (tribunal d'Utrecht) negou provimento ao pedido da Ryanair na medida em que era baseado na violação da Diretiva 96/9 e da lei sobre as bases de dados. Em contrapartida, deu provimento ao pedido enquanto baseado na Aw e condenou a PR Aviation a abster-se de qualquer violação dos direitos de autor da Ryanair sobre os seus dados de voos, bem como a indemnizá-la pelo prejuízo sofrido.
- 19 A PR Aviation interpôs recurso desta sentença. A Ryanair interpôs um recurso subordinado com o objetivo de contestar a apreciação do Rechtbank Utrecht segundo a qual ela não pode beneficiar da proteção prevista na Diretiva 96/9 e na lei sobre as bases de dados.
- 20 Por acórdão de 13 de março de 2012, o Gerechtshof te Amsterdam (Tribunal de Recurso de Amesterdão) anulou a sentença do Rechtbank Utrecht e negou provimento ao recurso subordinado interposto pela Ryanair.
- 21 Em substância, decidiu, no que diz respeito ao direito de autor, que, mesmo partindo do princípio de que as informações digitais tornadas públicas pela Ryanair estão abrangidas pela proteção dos escritos («geschriftenbescherming»), no sentido do artigo 10.º, n.º 1, 1º, da Aw, a PR Aviation não tinha infringido os direitos da Ryanair, dado que o seu comportamento correspondia a uma utilização normal, no sentido do artigo 24.ºa, n.º 1, da Aw, e, portanto, legítima, do sítio Internet da Ryanair. Acrescentou que a proibição, contida nas condições gerais da Ryanair, de utilizar o seu sítio Internet para fins comerciais não era suscetível de infirmar a conclusão anterior, tendo em conta, especialmente, o artigo 24.ºa, n.º 3, da Aw, que corresponde ao artigo 15.º da Diretiva 96/9.
- 22 No que diz respeito ao direito *sui generis*, o Gerechtshof te Amsterdam considerou que a Ryanair não tinha provado a existência de um «investimento substancial» na criação da sua coletânea de dados, no sentido da Diretiva 96/9 e da lei sobre as bases de dados.
- 23 A Ryanair interpôs recurso do acórdão do Gerechtshof te Amsterdam para o Hoge Raad der Nederlanden (Tribunal Supremo dos Países Baixos). Em apoio do seu recurso, invoca um único fundamento que está dividido em duas partes.
- 24 Na primeira parte do fundamento, a Ryanair critica a apreciação do Gerechtshof segundo a qual ela não pode beneficiar da proteção dos escritos, no sentido do artigo 10.º, n.º 1, 1º, da Aw.
- 25 A este respeito, o órgão jurisdicional de reenvio considera, todavia, que nenhum outro critério, a não ser o da originalidade, pode intervir para efeitos da proteção do direito de autor. Sublinhando que decorre do acórdão do Gerechtshof te Amsterdam que a coletânea de dados da Ryanair não cumpre este critério, concluiu que essa parte do fundamento suscitado pela Ryanair não pode levar à anulação desse acórdão.

- 26 Na segunda parte do seu fundamento de recurso, invocada a título subsidiário, a Ryanair alega, em substância, que foi sem razão que o Gerechtshof te Amsterdam considerou que o facto de a PR Aviation ter desobedecido à proibição contratual que lhe foi imposta, de extrair dados da base da Ryanair para fins comerciais sem ter celebrado um contrato de licença escrito com esta última sociedade, não era constitutivo de um incumprimento da PR Aviation.
- 27 A este respeito, o órgão jurisdicional de reenvio tem dúvidas quanto à questão de saber se o âmbito de aplicação da Diretiva 96/9 engloba as bases de dados que não são protegidas nem pelo direito de autor, ao abrigo do capítulo II da diretiva, nem pelo direito *sui generis*, ao abrigo do capítulo III da referida diretiva, e se, portanto, os limites à liberdade contratual que decorrem dos artigos 6.º, n.º 1, 8.º e 15.º da mesma diretiva são também válidos para essas bases de dados.
- 28 Nestas circunstâncias, o Hoge Raad der Nederlanden decidiu suspender a instância e submeter ao Tribunal de Justiça a seguinte questão prejudicial:

«O âmbito de aplicação da [Diretiva 96/9] inclui as bases de dados *online* que não são protegidas nem pelo direito de autor, ao abrigo do capítulo II [desta] diretiva, nem pelo direito *sui generis*, ao abrigo do capítulo III [da mesma diretiva], no sentido de que a liberdade de utilizar essas bases de dados, *ex vi* (ou mediante aplicação analógica) [dos] artigo[s] 6.º, n.º 1, e 8.º, em conjugação com o artigo 15.º [da Diretiva 96/9], não pode ser contratualmente limitada?»

#### Quanto à questão prejudicial

- 29 Através da sua questão, que assenta na premissa segundo a qual a coletânea de dados da Ryanair, em causa no processo principal, constitui uma base de dados na aceção do artigo 1.º, n.º 2, da Diretiva 96/9, que não é, contudo, protegida pelo direito de autor, ao abrigo do capítulo II desta diretiva, nem pelo direito *sui generis*, ao abrigo do capítulo III da mesma diretiva, o que compete ao órgão jurisdicional de reenvio verificar, este órgão pergunta, no essencial, se a Diretiva 96/9 deve ser interpretada no sentido de que, tendo em conta a aplicação conjugada dos seus artigos 6.º, n.º 1, 8.º e 15.º, a liberdade de utilizar essa base de dados não pode ser contratualmente limitada.
- 30 A título liminar, convém recordar que, em conformidade com jurisprudência constante, uma diretiva não pode, por si mesma, criar obrigações a um particular, nem, por conseguinte, ser invocada, enquanto tal, contra ele (v., designadamente, acórdãos Faccini Dori, C-91/92, EU:C:1994:292, n.º 20; Küçükdeveci, C-555/07, EU:C:2010:21, n.º 46; e Dominguez, C-282/10, EU:C:2012:33, n.º 37).
- 31 É igualmente jurisprudência constante que, ao aplicar o direito interno, os órgãos jurisdicionais nacionais são obrigados a interpretá-lo, na medida do possível, à luz do texto e da finalidade da diretiva em causa (v., designadamente, acórdãos Pfeiffer e o., C-397/01 a C-403/01, EU:C:2004:584, n.º 114; Küçükdeveci, EU:C:2010:21, n.º 48, e Dominguez, EU:C:2012:33, n.º 24).
- 32 Feitas estas precisões preliminares, convém salientar que, no capítulo I da Diretiva 96/9, o artigo 1.º, n.º 2, define o conceito de «base de dados».
- 33 Embora, como salienta a PR Aviation, a referida disposição confira a esse conceito um vasto âmbito, sem considerações de ordem formal, técnica ou material (v., neste sentido, acórdão Fixtures Marketing, C-444/02, EU:C:2004:697, n.º 20 à 32), também é um facto que a definição contida no artigo 1.º, n.º 2, da Diretiva 96/9 deve ser interpretada, segundo os seus próprios termos, «[p]ara efeitos da presente diretiva».
- 34 Ora, nos termos do artigo 1.º, n.º 1, da Diretiva 96/9, esta tem por objeto a «proteção jurídica das bases de dados». A este propósito, a diretiva institui duas formas de proteção jurídica destas bases. A primeira forma, regida pelos artigos 3.º a 6.º da referida diretiva, que fazem parte do seu capítulo II,

consiste na proteção pelo direito de autor e é aplicável, nos termos do artigo 3.º, n.º 1, da mesma diretiva, às bases de dados que, pela seleção ou disposição das matérias, constituam uma criação intelectual específica do respetivo autor. A segunda forma, regida pelos artigos 7.º a 11.º da Diretiva 96/9, que fazem parte do seu capítulo III, consiste na proteção por um direito *sui generis* e é aplicável, nos termos do artigo 7.º, n.º 1, da mesma diretiva, às bases de dados cuja obtenção, verificação ou apresentação do conteúdo representem um investimento substancial do ponto de vista qualitativo ou quantitativo. Estas duas formas de proteção jurídica são objeto de disposições comuns nos artigos 12.º a 16.º da referida diretiva, que fazem parte do seu capítulo IV.

- 35 Por conseguinte, a circunstância de uma base de dados corresponder aos elementos da definição contida no artigo 1.º, n.º 2, da Diretiva 96/9 não permite considerar, contrariamente ao que sustenta a PR Aviation, que lhe sejam aplicáveis as disposições dessa diretiva que regulam o direito de autor e/ou o direito *sui generis*, se ela não cumprir o requisito de aplicação da proteção pelo direito de autor previsto no artigo 3.º, n.º 1, da dita diretiva nem o requisito de aplicação da proteção pelo direito *sui generis* previsto no artigo 7.º, n.º 1, da mesma diretiva.
- 36 Quanto às disposições da Diretiva 96/9 especificamente referidas pelo órgão jurisdicional de reenvio na sua questão, convém acrescentar que o artigo 6.º, n.º 1, desta diretiva, que, sob determinadas condições, autoriza o utilizador legítimo de uma base de dados a efetuar, sem autorização do autor dessa base, os atos enumerados no artigo 5.º da dita diretiva, faz parte, como este último artigo, do capítulo da diretiva consagrado ao direito de autor e não é, por conseguinte, aplicável às bases de dados que não são protegidas por este direito.
- 37 O artigo 8.º da Diretiva 96/9, que prevê, designadamente, os direitos do utilizador legítimo de uma base de dados, figura, por seu turno, no capítulo da diretiva consagrado ao direito *sui generis* e não é, por conseguinte, aplicável às bases de dados que não são protegidas por este direito.
- 38 Quanto ao artigo 15.º da Diretiva 96/9, que consagra o caráter imperativo de certas disposições da mesma diretiva ao declarar nula qualquer disposição contratual contrária a estas, visa expressamente apenas os artigos 6.º, n.º 1, e 8.º da referida diretiva.
- 39 Resulta assim do objeto e da estrutura da Diretiva 96/9 que os seus artigos 6.º, n.º 1, 8.º e 15.º, que instituem direitos de caráter imperativo a favor dos utilizadores legítimos de uma base de dados, não são aplicáveis a uma base de dados que não é protegida pelo direito de autor nem pelo direito *sui generis*, previstos na diretiva, de modo que esta não se opõe à adoção de cláusulas contratuais que tenham por objeto as condições de utilização dessa base de dados.
- 40 Esta análise é corroborada pela economia geral da Diretiva 96/9. Como sublinharam a Ryanair e a Comissão Europeia, esta diretiva assenta num equilíbrio entre, por um lado, os direitos da pessoa que criou uma base de dados e, por outro, os direitos dos utilizadores legítimos dessa base de dados, concretamente, os terceiros autorizados por essa pessoa a utilizar a referida base. Neste contexto, a aplicação dos artigos 6.º, n.º 1, 8.º e 15.º da Diretiva 96/9, que conferem direitos a esses utilizadores legítimos e, dessa maneira, limitam os direitos da pessoa que criou a base de dados, só é possível com uma base de dados sobre a qual o seu criador dispõe de direitos ao abrigo do direito de autor reconhecido no artigo 5.º da mesma diretiva, ou do direito *sui generis* reconhecido no seu artigo 7.º Em contrapartida, não são aplicáveis se se tratar de uma base de dados cujo criador não usufrui, ao abrigo da Diretiva 96/9, de nenhum dos direitos anteriormente mencionados.
- 41 Contrariamente ao alegado pela PR Aviation, esta interpretação da Diretiva 96/9 não pode reduzir o interesse de reivindicar a proteção jurídica instituída pela referida diretiva, na medida em que o criador de uma base de dados protegida pela mesma diretiva não dispõe, diferentemente do criador de uma base de dados não protegida pela diretiva, da liberdade contratual de limitar os direitos dos utilizadores da sua base.

- 42 Com efeito, essa argumentação não tem em consideração o interesse jurídico e económico que o regime de proteção automática, harmonizado nos Estados-Membros, representa para a pessoa que investiu na criação de uma base de dados, que está ligado ao direito exclusivo, ao abrigo dos direitos de autor, de reservar para si os diferentes atos referidos no artigo 5.º da Diretiva 96/9, bem como ao direito de proibir, ao abrigo do direito *sui generis*, os atos previstos nos artigos 7.º, n.º 1 e 5, e 8.º, n.º 2, desta diretiva. Como a Comissão sublinhou na audiência, o benefício desta proteção não pressupõe o cumprimento de qualquer formalidade administrativa e não impõe nenhum compromisso convencional prévio.
- 43 Assim sendo, se o criador de uma base de dados protegida pela Diretiva 96/9 decidir autorizar a utilização da sua base de dados ou de uma cópia desta, poderá, como confirma o considerando 34 da diretiva, limitar essa utilização através de um contrato de licença celebrado com o utilizador legítimo, que precise, respeitando as disposições da dita diretiva, os «fins e [a] forma» de utilizar a referida base de dados ou a sua cópia.
- 44 Em contrapartida, tratando-se de uma base de dados à qual a Diretiva 96/9 não é aplicável, o seu criador não beneficia do regime de proteção jurídica instituído pela diretiva, de modo que apenas pode invocar uma proteção da sua base de dados com fundamento no direito nacional aplicável.
- 45 Tendo em conta todas as considerações precedentes, deve responder-se à questão colocada que a Diretiva 96/9 deve ser interpretada no sentido de que não é aplicável a uma base de dados que não é protegida pelo direito de autor nem pelo direito *sui generis* nos termos da diretiva, de modo que os artigos 6.º, n.º 1, 8.º e 15.º da diretiva não impedem o criador dessa base de dados de estabelecer limites contratuais à sua utilização por terceiros, sem prejuízo do direito nacional aplicável.

#### Quanto às despesas

- 46 Revestindo o processo, quanto às partes na causa principal, a natureza de incidente suscitado perante o órgão jurisdicional de reenvio, compete a este decidir quanto às despesas. As despesas efetuadas pelas outras partes para a apresentação de observações ao Tribunal de Justiça não são reembolsáveis.

Pelos fundamentos expostos, o Tribunal de Justiça (Segunda Secção) declara:

A Diretiva 96/9/CE do Parlamento Europeu e do Conselho, de 11 de março de 1996, relativa à proteção jurídica das bases de dados, deve ser interpretada no sentido de que não é aplicável a uma base de dados que não é protegida pelo direito de autor nem pelo direito *sui generis* nos termos da diretiva, de modo que os artigos 6.º, n.º 1, 8.º e 15.º da diretiva não impedem o criador dessa base de dados de estabelecer limites contratuais à sua utilização por terceiros, sem prejuízo do direito nacional aplicável.

Assinaturas

## ANEXO C – Análise Jurisprudencial Sobre Casos Envolvendo Bases de Dados (EUA)

### *Caso 1 – Pharmatrak*

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

In re PHARMATRAK, INC.  
PRIVACY LITIGATION

\*  
\*  
\*  
\*  
\*

Civil Action No. 00-11672-JLT  
MDL Docket No. 1400

MEMORANDUM

August 13, 2002

TAURO, J.,

Plaintiffs Rob Barring, Noah Blumofe, Jim Darby, Karen Gassman, Robin McClary, Harris Perlman, and Marcus Schroers (“Plaintiffs”) bring this consolidated action against Pharmatrak, Inc. (“Defendant Pharmatrak”)<sup>1</sup> and several pharmaceutical companies: Pfizer, Inc., Pharmacia Corporation, SmithKline Beecham Corporation, Glaxo Wellcome, Inc., and American Home Products Corporation (the “Pharmaceutical Defendants”). The Consolidated Amended Class Action Complaint alleges that Defendants secretly intercepted and accessed Plaintiffs’ personal information and Web browsing habits through the use of “cookies” and other devices, in violation of state and federal law.

The Parties’ cross-motions for summary judgment are now before the court.

**PROCEDURAL BACKGROUND**

Plaintiffs Blumofe and Gassman filed suit in this court on August 18, 2000. The remaining Plaintiffs filed complaints in the Southern District of New York. On April 18, 2001,

---

<sup>1</sup>Following the practice of the Parties, the court will refer solely to Pharmatrak in reference to the activities of both Pharmatrak and Glocal Communications, Ltd. (“Glocal”), the parent company of Pharmatrak.

---

the Judicial Panel on Multi-District Litigation issued an order transferring the six New York actions to the District of Massachusetts.

Plaintiffs filed the Amended Consolidated Class Action Complaint (“Complaint”) on June 28, 2001. In December 2001, the court held a scheduling conference and authorized the Plaintiffs to examine Defendant Pharmatrak’s computer servers. This limited discovery took place during December 2001 and January 2002 at Pharmatrak’s former corporate headquarters in Boston, Massachusetts.

Pursuant to the court’s March 26, 2002 Order, the Parties refiled motions for summary judgment. The court held a hearing on Defendants’ and Plaintiffs’ motions for summary judgment on July 24, 2002.

#### FACTUAL BACKGROUND

Plaintiffs allege that Defendants “secretly intercepted and accessed Internet users’ electronic communications with various health-related and medical-related Internet Web sites and secretly accessed their computer hard drives in order to collect private information about their Web browsing habits [and] confidential health information without their knowledge, authorization, or consent.”<sup>2</sup> Plaintiffs contend that the Pharmaceutical Defendants conspired with Plaintiff Pharmatrak to “collect and share this wrongfully obtained personal and sensitive information.”<sup>3</sup> This activity was allegedly accomplished through the use of “web bugs,” “persistent cookies,” and other devices.<sup>4</sup>

---

<sup>2</sup>Compl. ¶ 1.

<sup>3</sup>Id.

<sup>4</sup>Compl. ¶ 25.

The general principles of computers, the Internet, and the Web have been detailed elsewhere,<sup>5</sup> and because such facts are undisputed in this case, further elaboration is unnecessary. Analysis of the Parties' relationships in this case, however, requires a brief discussion of the specific methods by which the Parties communicated with each other, and the manner in which Defendants allegedly accessed and intercepted private information.

As stated in the Complaint, the Plaintiffs "access the Internet and communicate with other computers through use of commercial ISPs . . . or through computers known as 'servers' that are operated by the entity which provides their computer access, such as their employer. In each case, the ISP or the server provides the electronic communication service that allows the user's computer to connect with other computers on the Internet."<sup>6</sup> Plaintiffs assert that personal computers "can and sometimes do act as servers,"<sup>7</sup> but do not allege that any of the named Plaintiffs' computers were used in such a capacity.

The Pharmaceutical Defendants hired Defendant Pharmatrak to monitor their corporate web sites and provide monthly analysis of web site traffic.<sup>8</sup> Pharmatrak offered its clients two relevant products: NETcompare, which was designed to monitor activity across clients' web pages, and DRUGcompare, which was designed to monitor activity across disease categories and

---

<sup>5</sup>See Reno v. ACLU, 512 U.S. 844 (1997) (discussing the Internet); In re DoubleClick Inc. Privacy Litigation, 154 F.Supp.2d 497, 500-505 (S.D.N.Y. 2001) (discussing the Internet, the Web, cookies, and data collection).

<sup>6</sup>Compl. ¶ 40. "Servers" are computers which store documents and make them available over the Internet. See DoubleClick, 154 F.Supp.2d at 501. "ISPs" are Internet Service Providers.

<sup>7</sup>Pls.' Mem. of Law in Supp. of Mot. for Summ. J. 5.

<sup>8</sup>Compl. ¶ 47.

drug product pages.<sup>9</sup> All of the Pharmaceutical Defendants purchased NETcompare, and Defendant Pharmacia may have licensed DRUGcompare during testing phases.<sup>10</sup> Pharmatrak specifically represented to the Pharmaceutical Defendants that these products did not collect “personally identifiable information.”<sup>11</sup> Even though the Pharmaceutical Defendants may not have known precisely how Pharmatrak’s software worked, Plaintiffs readily admit that “the Pharmaceutical Defendants did authorize Pharmatrak’s presence upon their Web sites . . . .”<sup>12</sup>

Pharmatrak’s system operated through the use of HTML programming,<sup>13</sup> JavaScript programming,<sup>14</sup> cookies,<sup>15</sup> and “web bugs.”<sup>16</sup> Each of the Pharmaceutical Defendants’ web pages were programmed with Pharmatrak code, which allowed Pharmatrak to monitor web site activity.<sup>17</sup> When a computer browser requested information from a Pharmaceutical Defendant’s web page, the web page would send the requested information to the user, and the site’s programming code would instruct the user’s browser to contact Pharmatrak’s web server and

---

<sup>9</sup>Compl. ¶ 46.

<sup>10</sup>See Michael Sonnenreich Dep. (“M. Sonn. Dep.”) at 76:4, 84:4-8.

<sup>11</sup>See M. Sonn. Dep. at 93-95.

<sup>12</sup>Pls.’ Mem. of Law. in Opp. to Defs.’ Mot. for Summ. J. 6.

<sup>13</sup>“HTML” is “HyperText Markup Language.” As discussed in the Declaration of Matthew Curtin, HTML is “electronic document definition format typically used on the web. Web browsers read HTML to determine how to render an electronic document for presentation to the user.” Curtin Decl. ¶ 51.

<sup>14</sup>As discussed below, JavaScript is an Internet programming language.

<sup>15</sup>“Cookies” are electronic files, and are more fully discussed below.

<sup>16</sup>Compl. ¶ 49.

<sup>17</sup>Compl. ¶ 50.

retrieve a “clear GIF” from it.<sup>18</sup> A clear GIF is a one pixel-by-one pixel or two pixels-by-two pixels graphic image, and is sometimes called a web bug or a “pixel tag.”<sup>19</sup> The purpose of a clear GIF was to cause the user’s computer browser to communicate directly with Pharmatrak’s web server.<sup>20</sup> Some communications may have also included code referencing JavaApplet, a software program that runs in a user’s browser, or JavaScript, an Internet programming language.<sup>21</sup>

Having caused the user’s Internet browser to contact Pharmatrak, Pharmatrak then sent a cookie back to the browser.<sup>22</sup> A cookie is an electronic file “attached” to a user’s computer by a computer server. Plaintiffs concede that “[c]ookies generally perform many convenient and innocuous functions.”<sup>23</sup> Commonly, cookies are used to store users’ preferences and other information, which allows users to easily access and utilize personalized services on the web or to maintain an online “shopping cart.”<sup>24</sup> Cookies also allow web sites to differentiate between users as they visit by assigning each individual browser a unique, randomly generated numeric or alphanumeric identifier.<sup>25</sup> If an individual browser had already visited the “Pharmatrak-enabled” website, Pharmatrak would recognize the previously placed cookie and could therefore

---

<sup>18</sup>See *id.*

<sup>19</sup>Compl. ¶ 51.

<sup>20</sup>See *id.*

<sup>21</sup>See Pls.’ Mem. of Law in Supp. of Mot. for Summ. J. 12.

<sup>22</sup>Compl. ¶ 55.

<sup>23</sup>Compl. ¶ 56. See Declaration of C. Matthew Curtin (“Curtin Decl.”) ¶ 56.

<sup>24</sup>Compl. ¶ 56.

<sup>25</sup>Compl. ¶ 58.

---

differentiate between a repeat visit and an initial visit.<sup>26</sup> Pharmatrak programmed its cookies to expire after 90 days.<sup>27</sup> It is possible that many individual users were unaware that, in addition to their browser communicating with a Pharmaceutical Defendant's web site, it was also communicating with Pharmatrak.<sup>28</sup>

Plaintiffs allege that the JavaApplet used by Pharmatrak allowed Pharmatrak to monitor the length of time that a particular user viewed one of the Pharmaceutical Defendants' web pages.<sup>29</sup> Plaintiffs also allege that the JavaScript programming allowed Pharmatrak to "intercept the full URL<sup>30</sup> of the tracked Web page visited by the user," as well as "the full URL of the Web page visited by the Internet user *immediately prior* to the user's visit to the Pharmatrak-coded Web page. This prior Web page address is know as a 'referrer URL.'<sup>31</sup> According to Plaintiffs, Pharmatrak used JavaScript "to extract referring URLs from the client's history, thereby bypassing any security or privacy mechanisms put in place to control the flow of potentially sensitive data."<sup>32</sup> The JavaScript and JavaApplet, therefore, also caused users' computer browsers to communicate with Pharmatrak's server while they intentionally communicated with the Pharmaceutical Defendants' servers.

---

<sup>26</sup>Compl. ¶ 55.

<sup>27</sup>See Pls.' Mem. of Law in Supp. of Mot. for Summ. J. 13 n.8.

<sup>28</sup>Compl. ¶ 60.

<sup>29</sup>See Pls.' Mem. of Law in Supp. of Mot. for Summ. J. 13.

<sup>30</sup>A "URL" is a Uniform Resource Locator, which indicates the specific location of web documents on a server. Compl. ¶ 39.

<sup>31</sup>*Id.* at 14 (emphasis in original).

<sup>32</sup>Curtin Decl. ¶ 60.

In a subheading on page 21 of the Complaint, Plaintiffs also assert that Pharmatrak was able to "Capture [] Personal Information Submitted by Internet Users to the Pharmaceutical Defendants' Web Sites."<sup>49</sup> Users submitted this information in two ways. First, an individual could use the "POST" method, and voluntarily fill out an online form in order to register with the site, or to receive mailings, a rebate, or other information. For example, an individual wishing to view the full text of articles on [nytimes.com](http://nytimes.com) must first register with the site, a process which requires the individual to volunteer certain information.

Second, an individual using the "GET" method could perform an online search, resulting in a URL with search terms appended to it. The appended information is known as the "query string."<sup>50</sup> For example, a person interested in Cornell Law School could perform a search resulting in the following URL: <http://search.yahoo.com/bin/search?p=cornell+law+school>.<sup>51</sup> All of the material following the question mark (i.e. [p=cornell+law+school](http://search.yahoo.com/bin/search?p=cornell+law+school)) is known as the query string, and is "rich in useful content."<sup>52</sup> Plaintiffs allege that Pharmatrak was able to intercept and collect detailed, specific information about individual users from the full URLs, and place the information into relational databases.<sup>53</sup>

Plaintiffs' computer scientist, C. Matthew Curtin, and his company, Interhack, examined Pharmatrak's servers between December 17, 2001 and January 18, 2002, pursuant to the court's

---

<sup>49</sup>Compl. at 21.

<sup>50</sup>Compl. ¶ 70.

<sup>51</sup>See id.

<sup>52</sup>Pls.' Mem. of Law in Supp. of Mot. for Summ. J. 6.

<sup>53</sup>See id. at 7.

Order. The examination of Pharmatrak's logs "identified hundreds of people by name."<sup>48</sup> Based on Curtin's analysis, Plaintiffs claim that Pharmatrak collected information which included: names, addresses, telephone numbers, dates of birth, sex, insurance status, medical conditions, education levels, and occupations.<sup>49</sup> Pharmatrak also collected data about email communications, including user names, email addresses, and subject lines from emails.<sup>50</sup> Although Plaintiffs submit no evidence that Pharmatrak collected, sorted, or assembled this information into detailed "profiles," other than the aggregate information it submitted to the Pharmaceutical Defendants, Curtin did build such profiles.<sup>51</sup> Curtin also asserts that it would be possible to build detailed profiles of individuals using the data collected by Pharmatrak and matching it to "another data source, such as a telephone book."<sup>52</sup> Again, however, there is no evidence that Pharmatrak ever attempted to do so.

In sum, Plaintiffs argue that "Pharmatrak's technology permits defendants to collect extensive, detailed information about plaintiffs and Class members."<sup>53</sup> In addition to the personal information discussed above, the information collected allegedly included "Web sites the Internet users were at prior to the time they went to the Pharmaceutical Defendants' Web sites, questions they asked and typed in at those prior sites, information they entered while at the Pharmaceutical

---

<sup>48</sup>Curtin Decl. ¶ 53.

<sup>49</sup>See Curtin Decl. ¶ 18.

<sup>50</sup>See Curtin Decl. ¶ 90.

<sup>51</sup>See Curtin Decl. ¶ 19.

<sup>52</sup>See Curtin Decl. ¶ 19.

<sup>53</sup>Compl. ¶ 74.

Defendants' web sites, and the types of computers they were using."<sup>44</sup>

#### DISCUSSION

Under Federal Rule of Civil Procedure 56, summary judgment is appropriate "if the pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any, show that there is no genuine issue as to any material fact and that the moving party is entitled to a judgment as a matter of law."<sup>45</sup> Rule 56 mandates summary judgment "after adequate time for discovery and upon motion, against a party who fails to make a showing sufficient to establish the existence of an element essential to that party's case, and on which that party will bear the burden of proof at trial."<sup>46</sup>

The "party seeking summary judgment [must] make a preliminary showing that no genuine issue of material fact exists. Once the movant has made this showing, the nonmovant must contradict the showing by pointing to specific facts demonstrating that there is, instead, a trialworthy issue."<sup>47</sup> The party opposing summary judgment must produce specific evidence of a material factual dispute. The First Circuit has noted that "[a] genuine issue of material fact does not spring into being simply because a litigant claims that one exists. Neither wishful thinking nor 'mere promise[s] to produce admissible evidence at trial' . . . nor conclusory responses unsupported by evidence . . . will serve to defeat a properly focused Rule 56 motion."<sup>48</sup>

---

<sup>44</sup>Pls.' Mem. of Law. in Opp. to Defs.' Mot. for Summ. J. 4.

<sup>45</sup>Fed. R. Civ. P. 56(c).

<sup>46</sup>Celotex Corp. v. Catrett, 477 U.S. 317, 322 (1986).

<sup>47</sup>Blackie v. State of ME, 75 F.3d 716, 721 (1<sup>st</sup> Cir. 1996) (quotations omitted).

<sup>48</sup>Griggs-Ryan v. Smith, 904 F.2d 112, 115 (1<sup>st</sup> Cir. 1990) (citations omitted).

The Parties file cross-motions for summary judgment. “The happenstance that all parties seek summary judgment neither alters the yardstick nor empowers the trial court to resolve authentic disputes anent material facts.”<sup>19</sup> A court considering cross-motions for summary judgment must consider “each motion separately, being careful to draw inferences against each movant in turn.”<sup>20</sup>

Plaintiffs seek summary judgment against Defendants Pharmatrak and Global, and Defendants each seek summary judgment against Plaintiffs.

**A. Court I- The Wiretap Act**<sup>21</sup>

Title I of the Electronic Communication Privacy Act of 1986 (“ECPA”), Interception of Electronic Communications (“The Wiretap Act”), provides that:

Except as otherwise specifically provided in this chapter[,] any person who – (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept, any wire, oral, or electronic communication . . . shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).<sup>22</sup>

This criminal statute provides for a private right of action, and is subject the following statutory exception:

(d) It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of

---

<sup>19</sup>Id.

<sup>20</sup>Id.

<sup>21</sup>18 U.S.C. § 2510, *et seq.*

<sup>22</sup>18 U.S.C. § 2511(1)(a).

committing any criminal or tortious act . . . .<sup>18</sup>

Plaintiffs argue that Defendants intentionally “intercepted plaintiffs’ or Class members’ electronic communications with the Web sites they visited without plaintiffs’ or the Class’ [sic] knowledge, authorization, or consent. . . .”<sup>19</sup>

#### 1. Pharmaceutical Defendants

After Defendants had fully briefed the issue, Plaintiffs’ counsel orally informed the court at the summary judgment hearing that Plaintiffs would withdraw the Wiretap Act claim as it relates to the Pharmaceutical Defendants.<sup>20</sup> Count I is therefore DISMISSED with regard to these defendants.

#### 2. Pharmatrak

Plaintiffs claim that “Pharmatrak intercepted plaintiffs’ transmission of their personal information to the Pharmaceutical Defendants’ Web sites without the express or implied consent of either plaintiffs or the Pharmaceutical Defendants.”<sup>21</sup> Despite the fact that the Pharmaceutical Defendants may have consented to Pharmatrak’s assembly of anonymous, aggregate information, Plaintiffs insist that the web sites never consented to Pharmatrak’s collection of personally identifiable information.<sup>22</sup> Absent this specific consent, Plaintiffs argue, the Wiretap Act’s

---

<sup>18</sup>18 U.S.C. § 2511(2)(d).

<sup>19</sup>Compl. ¶ 95.

<sup>20</sup>Plaintiffs’ counsel stated that “I don’t think the plaintiffs have a claim under the wiretap statute against the pharmaceutical defendants,” and indicated that Plaintiffs would withdraw the claim. Hearing Tr. 66:20-22 (July 24, 2002).

<sup>21</sup>Pls.’ Mem. of Law in Supp. of Mot. for Summ. J. 20.

<sup>22</sup>See *id.*

statutory exception simply does not apply.

Pharmatrak concedes that the Pharmaceutical Defendants did not consent to the collection of personally identifiable information.<sup>88</sup> According to Pharmatrak, however, the relevant inquiry is whether the Pharmaceutical Defendants consented to Pharmatrak's NETcompare service, i.e. the collection of data from the Pharmaceutical Defendants' web sites, regardless of how the service eventually operated.<sup>89</sup> It is undisputed that the Pharmaceutical Defendants contracted with Defendant Pharmatrak to obtain data regarding their web sites, and that they proceeded to have the Pharmatrak code placed on the web sites. Pharmatrak, therefore, asserts that the statutory exception for consent has been met, and that it is entitled to summary judgment on the Wiretap Act claim.

In *In re DoubleClick Inc. Privacy Litigation* ("DoubleClick"),<sup>90</sup> the Southern District of New York disposed of a multidistrict consolidated class action case pursuant to Rule 12(b)(6). There, the plaintiffs alleged that DoubleClick, an Internet advertising firm, placed cookies on their computers, thereby collecting "information that Web users, including plaintiffs and the Class, consider to be personal and private, such as names, e-mail addresses, home and business addresses, telephone numbers, searches performed on the Internet, Web pages or sites visited on the Internet, and other communications and information that users would not ordinarily expect advertisers to be able to collect."<sup>91</sup>

---

<sup>88</sup>See Pharmatrak's Substitute Reply Mem. of Law in Supp. of Mot. for Summ. J. 8.

<sup>89</sup>See *id.* at 8-9.

<sup>90</sup>154 F.Supp.2d 497 (S.D.N.Y. 2001).

<sup>91</sup>*Id.* at 503.

The DoubleClick court found that the web sites affiliated with DoubleClick were “parties to the communication[s]” from plaintiffs and have given sufficient consent to DoubleClick to intercept them,<sup>62</sup> despite the possibility that the plaintiffs may not have known that their computers were communicating with DoubleClick, and that the affiliated Web sites may not have fully understood the mechanisms of the DoubleClick service.

Having found consent, the DoubleClick court proceeded to analyze Section 2511(2)(d)’s “criminal” or “tortious” purpose requirement, which “is to be construed narrowly.”<sup>63</sup> The court noted that the evidence in the case suggested that DoubleClick’s actions were motivated by legitimate business goals, and found an “utter lack of evidence that [DoubleClick’s] intent was tortious . . . .”<sup>64</sup> Because it found that DoubleClick acted with consent and without a tortious or criminal purpose, the court dismissed the plaintiffs’ Wiretap Act claim.<sup>65</sup>

In Chance v. Avenue A, Inc.,<sup>66</sup> the plaintiffs alleged that Avenue A had placed cookies on their computers, thus permitting the company to surreptitiously monitor plaintiffs’ electronic communications. First, addressing consent, the court held that “[i]t is implicit in the web pages’ code instructing the user’s computer to contact Avenue A, either directly or via DoubleClick’s server, that the web pages have consented to Avenue A’s interception of the communication

---

<sup>62</sup>Id. at 514, quoting 18 U.S.C. 2511(2)(d).

<sup>63</sup>See id. at 515-19.

<sup>64</sup>Id. at 519.

<sup>65</sup>See id.

<sup>66</sup>165 F.Supp.2d 1153 (W.D. Wash. 2001).

between them and the individual user.<sup>467</sup> The court also found that the plaintiffs had presented no evidence that the defendants acted with a tortious or illegal purpose and, therefore, granted summary judgment on the claim to Avenue A.<sup>468</sup>

In the present case, Plaintiffs concede that the Pharmaceutical Defendants consented to the placement of code for Pharmatrak's NETcompare service on their web sites.<sup>469</sup> As was the case in DoubleClick and Avenue A, the web site Defendants (here, the Pharmaceutical Defendants) consented to the service of a web-monitoring company (Pharmatrak), and such consent precludes a claim under the Wiretap Act. The Pharmaceutical companies contracted with Pharmatrak, and authorized Pharmatrak to communicate with any users who contacted the Pharmaceutical Web sites. Despite Plaintiffs' valiant attempts to shift the inquiry, it is irrelevant for the purposes of the Wiretap Act whether the Pharmaceutical Defendants knew the precise mechanisms of Pharmatrak's service or not. It is sufficient that the Pharmaceutical Defendants were parties to communications with Plaintiffs and consented to the monitoring service provided by Defendant Pharmatrak.

Plaintiffs are also unable to demonstrate that Defendants acted with a tortious purpose. Plaintiffs have produced no evidence "either (1) that the primary motivation, or (2) that a determinative factor in the actor [Pharmatrak's] motivation for intercepting the conversation was

---

<sup>467</sup>Id. at 1162.

<sup>468</sup>See id. at 1163.

<sup>469</sup>See Compl. ¶¶ 1-3.

to commit a criminal [or] tortious . . . act.”<sup>70</sup> Without a showing of the requisite *mens rea*, Plaintiffs cannot succeed on their claim under the Wiretap Act.

Because the Pharmaceutical Defendants consented to Pharmatrak’s NETcompare service, and because Plaintiffs are unable to present any evidence whatsoever of a tortious intent, Defendants are entitled to summary judgment on Count I of the Complaint.

**B. Count II - Stored Communications Act<sup>71</sup>**

Title II of the ECPA, also known as the “Stored Wire and Electronic Communications and Transactional Records Act,” “aims to prevent hackers from obtaining, altering, or destroying certain stored electronic communications.”<sup>72</sup> The statute provides:

[W]hoever – (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided by subsection (b) of this section.<sup>73</sup>

Plaintiffs acknowledge that § 2701 was primarily designed to provide a cause of action against computer hackers,<sup>74</sup> and argue that “Defendants’ conduct of accessing data in plaintiffs’ computers, including the content of plaintiffs’ e-mails, constitutes electronic trespassing and falls

---

<sup>70</sup>DoubleClick, 154 F.Supp.2d at 514-15, quoting United States v. Dale, 991 F.2d 819, 841-42 (D.C. Cir. 1993).

<sup>71</sup>18 U.S.C. § 2701, *et seq.*

<sup>72</sup>DoubleClick, 154 F.Supp.2d at 507.

<sup>73</sup>18 U.S.C. § 2701(a).

<sup>74</sup>See Pls.’ Mem. of Law in Opp’n to Defs.’ Mots. for Summ. J. 27.

squarely within the ambit of Section 2701.”<sup>53</sup>

Defendants disagree, and claim that they are entitled to summary judgment on at least two separate grounds: (1) Plaintiffs’ computers are not facilities which provide electronic communications services, an essential element of § 2701; and (2) any alleged access to “communications” was authorized.<sup>54</sup>

Defendants are correct that an individual Plaintiff’s personal computer is not a “facility through which an electronic communication service is provided” for the purposes of § 2701. Plaintiffs find it noteworthy that “[p]ersonal computers provide consumers with the opportunity to access the Internet and send or receive electronic communications,” and that “[w]ithout personal computers, most consumers would not be able to access the Internet or electronic communications.” Fair enough, but without a telephone, most consumers would not be able to access telephone lines, and without televisions, most consumers would not be able to access cable television. Just as telephones and televisions are necessary devices by which consumers access particular services, personal computers are necessary devices by which consumers connect to the Internet. While it is possible for modern computers to perform server-like functions, there is no evidence that any of the Plaintiffs used their computers in this way. While computers and telephones certainly provide services in the general sense of the word, that is not enough for the purposes of the ECPA. The relevant service is Internet access, and the service is provided through

---

<sup>53</sup>*Id.* at 28.

<sup>54</sup>*See* Mem. of Law in Supp. of Def. AHP’s Mot. for Summ. J. 21.

ISPs or other servers, not though Plaintiffs' PCs.<sup>77</sup>

Even if the court were to assume that Plaintiffs' computers are "facilities" under § 2701,<sup>78</sup> any access to stored communications was authorized and, thus, Defendants' conduct falls under the exception from liability created by § 2701(c)(2). As was the case in DoubleClick and Avenue A, the Pharmaceutical Defendants are "users" under the ECPA.<sup>79</sup> The DoubleClick court noted that, "in a practical sense, Web sites are among the most active 'users' of Internet access."<sup>80</sup> As users, the Pharmaceutical Defendants could consent to Pharmatrak's interception of Plaintiffs' communications, and Plaintiffs cannot survive the motions for summary judgment "based solely on the naked allegation that defendant[s'] access was 'unauthorized.'"<sup>81</sup>

Plaintiffs argue that this case is factually different from DoubleClick, because the Pharmaceutical Defendants did not know that Pharmatrak would collect the type and amount of personally identifiable information that it did. Even viewing this factual distinction in the light most favorable to Plaintiffs, the Pharmaceutical Defendants nonetheless authorized Pharmatrak to

---

<sup>77</sup>See DoubleClick, 154 F.Supp.2d at 508 ("Therefore, the 'service which provides to users thereof the ability to send or receive wire or electronic communications' is 'Internet access.'")

<sup>78</sup>The court in Avenue A found it "possible to conclude that modern computers, which serve as a conduit for the web server's communication to Avenue A, are facilities under the Act." Avenue A, 163 F.Supp.2d at 1161.

<sup>79</sup>See DoubleClick, 154 F.Supp.2d at 509 ("Therefore, we find as a matter of law that the DoubleClick-affiliated Web sites are 'users' of Internet access under the ECPA."); Avenue A, 163 F.Supp.2d at 1161 (finding that "at minimum the web site is a 'user' of that communication service").

<sup>80</sup>DoubleClick, 154 F.Supp.2d at 509.

<sup>81</sup>Id.

---

monitor electronic communications between the web sites and Plaintiffs. As discussed above in Part A.2, the Pharmaceutical Defendants consented to the monitoring service provided by Defendant Pharmatrak in NETcompare, even if they were unaware that the program was able to identify personal information.

In addition, the ECPA does not prohibit Pharmatrak's actions with regard to the placing of cookies on Plaintiffs' computers. Section § 2701 seeks to target communications which are in "electronic storage" incident to their transmission. This court agrees with the DoubleClick court that "Title II only protects electronic communications stored 'for a limited time' in the 'middle' of a transmission, i.e. when an electronic communication service temporarily stores a communication while waiting to store it."<sup>82</sup> Even if such cookies were covered by the ECPA, Pharmatrak created and sent the cookies, and thus any accessing of the cookies by Pharmatrak at a later date would certainly be "authorized." Because Pharmatrak's cookies fall outside the scope of § 2701, Plaintiffs' claim under that section must fail.

Finally, Plaintiffs persistently argue that the Pharmaceutical Defendants did not consent to the allegedly improper interception of personal information. If the Pharmaceutical Defendants did not consent to the alleged interception of personally identifiable information, then they could not have "intentionally access[ed] without authorization" any electronic communications. Without the necessary intent under this punitive statute, the Pharmaceutical Defendants cannot be held liable and are entitled to summary judgment.

Accordingly, all Defendants are entitled to summary judgment on Count II.

---

<sup>82</sup>DoubleClick, 154 F.Supp.2d at 512.

C. Count III - Computer Fraud and Abuse Act<sup>61</sup>

The Computer Fraud and Abuse Act (CFAA) creates a claim against:

(a) Whoever – . . . (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . (c) information from any protected computer if the conduct involved an interstate or foreign communication . . .<sup>62</sup>

The CFAA limits recovery to those persons who suffer “damage or loss by reason of a violation” of the Act. Section 1030(e)(8) defines damage as “any impairment to the integrity or availability of data, a program, a system, or information, that – (A) causes loss aggregating at least \$5,000 in value during any 1-year period to one or more individuals. . . .”<sup>63</sup>

Plaintiffs do not allege that their computers were physically damaged in any way, or that they suffered any damage resulting from the repair or replacement of their computer systems. Instead, Plaintiffs argue that their “sensible interpretation” of the CFAA allows recovery for a “cognizable ‘loss,’” as distinct from economic damage, for the invasion of their privacy and the “concomitant loss of control over the dissemination of their private information.”<sup>64</sup> Plaintiffs stress that they allege both loss and damages, and that the damage threshold of \$5,000 may be met by aggregating claims among individuals and over a one year period.

The CFAA does not define “loss,” and the First Circuit noted in EF Cultural Travel BV, et. al. v. Explorica<sup>65</sup> that “[f]ew courts have endeavored to resolve the contours of damage and

---

<sup>61</sup>18 U.S.C. § 1030.

<sup>62</sup>18 U.S.C. § 1030(a)(2).

<sup>63</sup>18 U.S.C. 1030(e)(8).

<sup>64</sup>Pls.’ Mem. of Law in Opp’n to Defs.’ Mot. for Summ. J. 38.

<sup>65</sup>274 F.3d 577 (1<sup>st</sup> Cir. 2001).

loss under the CFAA.<sup>88</sup> In that case, the First Circuit explicitly agreed with the DoubleClick court, and concluded that the statute's use of "damage or loss" indicated a Congressional desire to allow recovery for more than purely physical damage.<sup>89</sup> The First Circuit was careful to note, however, that it did not hold that any loss is compensable, and that "Congress could not have intended other types of loss to support recovery unless [the \$5,000] threshold were met."<sup>90</sup>

Plaintiffs have not shown any evidence whatsoever that Defendants have caused them at least \$5,000 of damage or loss. Even accepting Mr. Curtin's bald assertion that "[d]ata about people are valuable, marketable assets,"<sup>91</sup> Plaintiffs are unable to meet the statutory threshold. Any damage or loss under the CFAA may be aggregated across victims and across time, but only for a single act.<sup>92</sup> Because Plaintiffs have not shown any facts that demonstrate damage or loss of over \$5,000 for any single act of the Defendants, Defendants are entitled to summary judgment on Count III.<sup>93</sup>

#### CONCLUSION

For the foregoing reasons, Defendants' Motions for Summary Judgment [Docket #'s 139,

---

<sup>88</sup>Id. at 584.

<sup>89</sup>See id. at 585.

<sup>90</sup>Id.

<sup>91</sup>Curtin Decl. ¶ 13.

<sup>92</sup>See DoubleClick, 154 F.Supp.2d at 523; Avenue A, 165 F.Supp.2d at 1158. But see In re America Online, Inc., 168 F.Supp.2d 1359, 1374-75 (S.D. Fla. 2001).

<sup>93</sup>Even if Plaintiffs were able to establish damage or loss greater than the \$5,000 statutory threshold, Plaintiffs have produced no evidence that the Pharmaceutical Defendants possessed the requisite *mens rea* to be held liable under the CFAA.

143, 218, and 224] are ALLOWED as to Counts I, II, and III of the Consolidated Amended Class Action Complaint, and Plaintiffs' Motion for Summary Judgment [Docket # 237] is DENIED. Defendant Pharmatrak's Motion to Dismiss [Docket # 269 ] is DENIED.

Having granted summary judgment on Counts I, II, and III, this court declines to retain jurisdiction over Counts IV-IX, and those counts are DISMISSED, without prejudice.

AN ORDER WILL ISSUE.

---

United States District Judge



## Caso 2–Viacom

## VIACOM INTERNATIONAL, INC. v. YOUTUBE, INC.

676 F.3d 19

United States Court of Appeals, Second Circuit.

Decided: April 5, 2012.

- 7 JOSÉ A. CABRANES, Circuit Judge:
- 8 This appeal requires us to clarify the contours of the “safe harbor” provision of the Digital Millennium Copyright Act (DMCA) that limits the liability of online service providers for copyright infringement that occurs “by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider.” 17 U.S.C. § 512(c).[1]
- 9 The plaintiffs-appellants in these related actions—Viacom International, Inc. (“Viacom”), The Football Association Premier League Ltd. (“Premier League”), and various film studios, television networks, music publishers, and sports leagues (jointly, [676 F.3d 26] the “plaintiffs”)[2] —appeal from an August 10, 2010 judgment of the United States District Court for the Southern District of New York (Louis L. Stanton, Judge), which granted summary judgment to defendants-appellees YouTube, Inc., YouTube, LLC, and Google Inc. (jointly, “YouTube” or the “defendants”). The plaintiffs alleged direct and secondary copyright infringement based on the public performance, display, and reproduction of approximately 79,000 audiovisual “clips” that appeared on the YouTube website between 2005 and 2008. They demanded, *inter alia*, statutory damages pursuant to 17 U.S.C. § 504(c) or, in the alternative, actual damages from the alleged infringement, as well as declaratory and injunctive relief.[3]
- 10 In a June 23, 2010 Opinion and Order (the “June 23 Opinion”), the District Court held that the defendants were entitled to DMCA safe harbor protection primarily because they had insufficient notice of the particular infringements in suit. *Viacom Int’l, Inc. v. YouTube, Inc.*, 718 F.Supp.2d 514, 529 (S.D.N.Y.2010). In construing the statutory safe harbor, the District Court concluded that the “actual knowledge” or “aware[ne]ss of facts or circumstances” that would disqualify an online service provider from safe harbor protection under § 512(c)(1)(A) refer to “knowledge of specific and identifiable infringements.” [...] The District Court further held that item-specific knowledge of infringing activity is required for a service provider to have the “right and ability to control” infringing activity under § 512(c)(1)(B). [...] Finally, the District Court held that the replication, transmittal, and display of videos on YouTube constituted activity “by reason of the storage at the direction of a user” within the meaning of § 512(c)(1). [...]
- 11 These related cases present a series of significant questions of statutory construction. We conclude that the District Court correctly held that the § 512(c) safe harbor requires knowledge or awareness of specific infringing activity, but we vacate the order granting summary judgment because a reasonable jury could find that YouTube had actual knowledge or awareness of specific infringing activity on its website. We further hold that the District Court erred by interpreting the “right and ability to control” provision to require “item-specific” knowledge. Finally, we affirm the District Court’s holding that three of the challenged YouTube software functions fall within the safe harbor for

infringement that occurs “by reason of” user storage; we remand for further fact-finding with respect to a fourth software function.

## BACKGROUND

### A. The DMCA Safe Harbors

- 14 “The DMCA was enacted in 1998 to implement the World Intellectual Property Organization Copyright Treaty,” *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 440 (2d Cir.2001), and to update domestic copyright law for the digital age, [676 F.3d 27] [...]. Title II of the DMCA, separately titled the “Online Copyright Infringement Liability Limitation Act” (OCILLA), was designed to “clarif[y] the liability faced by service providers who transmit potentially infringing material over their networks.” [...] But “[r]ather than embarking upon a wholesale clarification” of various copyright doctrines, Congress elected “to leave current law in its evolving state and, instead, to create a series of ‘safe harbors[.]’ for certain common activities of service providers.” [...] To that end, OCILLA established a series of four “safe harbors” that allow qualifying service providers to limit their liability for claims of copyright infringement based on (a) “transitory digital network communications,” (b) “system caching,” (c) “information residing on systems or networks at [the] direction of users,” and (d) “information location tools.” 17 U.S.C. § 512(a)-(d).
- 15 To qualify for protection under any of the safe harbors, a party must meet a set of threshold criteria. First, the party must in fact be a “service provider,” defined, in pertinent part, as “a provider of online services or network access, or the operator of facilities therefor.” 17 U.S.C. § 512(k)(1)(B). A party that qualifies as a service provider must also satisfy certain “conditions of eligibility,” including the adoption and reasonable implementation of a “repeat infringer” policy that “provides for the termination in appropriate circumstances of subscribers and account holders of the service provider’s system or network.” *Id.* § 512(i)(1)(A). In addition, a qualifying service provider must accommodate “standard technical measures” that are “used by copyright owners to identify or protect copyrighted works.” *Id.* § 512(i)(1)(B), (i)(2).
- 16 Beyond the threshold criteria, a service provider must satisfy the requirements of a particular safe harbor. In this case, the safe harbor at issue is § 512(c), which covers infringement claims that arise “by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider.” *Id.* § 512(c)(1). The § 512(c) safe harbor will apply only if the service provider:
- 17 (A) (i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing;
- (ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or
- (iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;
- (B) does not receive a financial benefit directly attributable to the infringing activity,

in a case in which the service provider has the right and ability to control such activity; and

(C) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.

18 *Id.* § 512(c)(1)(A)-(C). Section 512(c) also sets forth a detailed notification scheme that requires service providers to “designate[ ] an agent to receive notifications of claimed infringement,” *id.* § 512(c)(2), and specifies the components of a proper notification, commonly known as a “takedown notice,” to that agent, see *id.* § 512(c)(3). Thus, actual knowledge of infringing material, awareness of facts or circumstances that make infringing activity apparent, or [676 F.3d 28] receipt of a takedown notice will each trigger an obligation to expeditiously remove the infringing material.

19 With the statutory context in mind, we now turn to the facts of this case.

#### B. Factual Background

21 YouTube was founded in February 2005 by Chad Hurley (“Hurley”), Steve Chen (“Chen”), and Jawed Karim (“Karim”), three former employees of the internet company PayPal. When YouTube announced the “official launch” of the website in December 2005, a press release described YouTube as a “consumer media company” that “allows people to watch, upload, and share personal video clips at [www.YouTube.com](http://www.YouTube.com).” Under the slogan “Broadcast yourself,” YouTube achieved rapid prominence and profitability, eclipsing competitors such as Google Video and Yahoo Video by wide margins. In November 2006, Google acquired YouTube in a stock-for-stock transaction valued at \$1.65 billion. By March 2010, at the time of summary judgment briefing in this litigation, site traffic on YouTube had soared to more than 1 billion daily video views, with more than 24 hours of new video uploaded to the site every minute.

22 The basic function of the YouTube website permits users to “upload” and view video clips free of charge. Before uploading a video to YouTube, a user must register and create an account with the website. The registration process requires the user to accept YouTube’s Terms of Use agreement, which provides, *inter alia*, that the user “will not submit material that is copyrighted ... unless [he is] the owner of such rights or ha[s] permission from their rightful owner to post the material and to grant YouTube all of the license rights granted herein.” When the registration process is complete, the user can sign in to his account, select a video to upload from the user’s personal computer, mobile phone, or other device, and instruct the YouTube system to upload the video by clicking on a virtual upload “button.”

23 Uploading a video to the YouTube website triggers a series of automated software functions. During the upload process, YouTube makes one or more exact copies of the video in its original file format. YouTube also makes one or more additional copies of the video in “Flash” format,<sup>[4]</sup> a process known as “transcoding.” The transcoding process ensures that YouTube videos are available for viewing by most users at their request. The YouTube system allows users to gain access to video content by “streaming” the video to

the user's computer in response to a playback request. YouTube uses a computer algorithm to identify clips that are "related" to a video the user watches and display links to the "related" clips.

### C. Procedural History

- 25 Plaintiff Viacom, an American media conglomerate, and various Viacom affiliates filed suit against YouTube on March 13, 2007, alleging direct and secondary copyright infringement<sup>[5]</sup> based on the public performance, display, and reproduction of their audiovisual works on the YouTube website. Plaintiff Premier League, an English soccer league, and Plaintiff Bourne Co. filed a putative class action against <sup>[676 F.3d 29]</sup> YouTube on May 4, 2007, alleging direct and secondary copyright infringement on behalf of all copyright owners whose material was copied, stored, displayed, or performed on YouTube without authorization. Specifically at issue were some 63,497 video clips identified by Viacom, as well as 13,500 additional clips (jointly, the "clips-in-suit") identified by the putative class plaintiffs.
- 26 The plaintiffs in both actions principally demanded statutory damages pursuant to 17 U.S.C. § 504(c) or, in the alternative, actual damages plus the defendants' profits from the alleged infringement, as well as declaratory and injunctive relief.<sup>[6]</sup> Judge Stanton, to whom the Viacom action was assigned, accepted the Premier League class action as related. At the close of discovery, the parties in both actions cross-moved for partial summary judgment with respect to the applicability of the DMCA safe harbor defense.<sup>[7]</sup>
- 27 In the dual-captioned June 23 Opinion, the District Court denied the plaintiffs' motions and granted summary judgment to the defendants, finding that YouTube qualified for DMCA safe harbor protection with respect to all claims of direct and secondary copyright infringement. [...] The District Court prefaced its analysis of the DMCA safe harbor by holding that, based on the plaintiffs' summary judgment submissions, "a jury could find that the defendants not only were generally aware of, but welcomed, copyright-infringing material being placed on their website." [...] However, the District Court also noted that the defendants had properly designated an agent pursuant to § 512(c)(2), and "when they received specific notice that a particular item infringed a copyright, they swiftly removed it." [...] Accordingly, the District Court identified the crux of the inquiry with respect to YouTube's copyright liability as follows:
- 28 [T]he critical question is whether the statutory phrases "actual knowledge that the material or an activity using the material on the system or network is infringing," and "facts or circumstances from which infringing activity is apparent" in § 512(c)(1)(A)(i) and (ii) mean a general awareness that there are infringements (here, claimed to be widespread and common), or rather mean actual or constructive knowledge of specific and identifiable infringements of individual items.
- 29 [...] After quoting at length from the legislative history of the DMCA, the District Court held that "the phrases 'actual knowledge that the material or an activity' is infringing, and 'facts or circumstances' indicating infringing activity, describe knowledge of specific and identifiable infringements of particular individual items." [...] "Mere knowledge of [the] prevalence of such activity in general," the District Court concluded, "is not enough." [...]

- 30 In a final section labeled “Other Points,” the District Court rejected two additional claims. First, it rejected the plaintiffs’ argument that the replication, transmittal and display of YouTube videos are functions that fall outside the protection § 512(c)(1) affords for “infringement of copyright by reason of ... storage at the direction of the user.” [...] Second, it rejected the plaintiffs’ argument [676 F.3d 30] that YouTube was ineligible for safe harbor protection under the control provision, holding that the “right and ability to control” infringing activity under § 512(c)(1)(B) requires “item-specific” knowledge thereof, because “the provider must know of the particular case before he can control it.” [...]
- 31 Following the June 23 Opinion, final judgment in favor of YouTube was entered on August 10, 2010. These appeals followed.

#### DISCUSSION

- 33 We review an order granting summary judgment de novo, drawing all factual inferences in favor of the non-moving party. [...] “Summary judgment is proper only when, construing the evidence in the light most favorable to the non-movant, ‘there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law.’” [...]

##### A. Actual and “Red Flag” Knowledge: § 512(c)(1)(A)

- 35 The first and most important question on appeal is whether the DMCA safe harbor at issue requires “actual knowledge” or “aware[ness]” of facts or circumstances indicating “specific and identifiable infringements,” [...]. We consider first the scope of the statutory provision and then its application to the record in this case.
- 36 **1. The Specificity Requirement**
- 37 “As in all statutory construction cases, we begin with the language of the statute,” [...] Under § 512(c)(1)(A), safe harbor protection is available only if the service provider:
- 38 (i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing;
- (ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or
- (iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material....
- 39 17 U.S.C. § 512(c)(1)(A). As previously noted, the District Court held that the statutory phrases “actual knowledge that the material ... is infringing” and “facts or circumstances from which infringing activity is apparent” refer to “knowledge of specific and identifiable infringements.” [...] For the reasons that follow, we substantially affirm that holding.

- 40 Although the parties marshal a battery of other arguments on appeal, it is the text of the statute that compels our conclusion. In particular, we are persuaded that the basic operation of § 512(c) requires knowledge or awareness of specific infringing activity. Under § 512(c)(1)(A), knowledge or awareness alone does not disqualify the service provider; rather, the provider that gains knowledge or awareness of infringing activity retains safe-harbor protection if it “acts expeditiously to remove, or disable access to, the material.” 17 U.S.C. § 512(c)(1)(A)(iii). Thus, the nature of the removal obligation itself contemplates knowledge or awareness of specific infringing material, because expeditious removal is possible only if the service provider knows with particularity which items to remove. Indeed, to require expeditious removal in the absence of specific knowledge [676 F.3d 31] or awareness would be to mandate an amorphous obligation to “take commercially reasonable steps” in response to a generalized awareness of infringement. [...] Such a view cannot be reconciled with the language of the statute, which requires “expeditious[ ]” action to remove or disable “the material” at issue. 17 U.S.C. § 512(c)(1)(A)(iii) (emphasis added).
- 41 On appeal, the plaintiffs dispute this conclusion by drawing our attention to § 512(c)(1)(A)(ii), the so-called “red flag” knowledge provision. See *id.* § 512(c)(1)(A)(ii) (limiting liability where, “in the absence of such actual knowledge, [the service provider] is not aware of facts or circumstances from which infringing activity is apparent”). In their view, the use of the phrase “facts or circumstances” demonstrates that Congress did not intend to limit the red flag provision to a particular type of knowledge. The plaintiffs contend that requiring awareness of specific infringements in order to establish “aware[ne]ss of facts or circumstances from which infringing activity is apparent,” 17 U.S.C. § 512(c)(1)(A)(ii), renders the red flag provision superfluous, because that provision would be satisfied only when the “actual knowledge” provision is also satisfied. For that reason, the plaintiffs urge the Court to hold that the red flag provision “requires less specificity” than the actual knowledge provision. [...]
- 42 This argument misconstrues the relationship between “actual” knowledge and “red flag” knowledge. It is true that “we are required to ‘disfavor interpretations of statutes that render language superfluous.’” [...] But contrary to the plaintiffs’ assertions, construing § 512(c)(1)(A) to require actual knowledge or awareness of specific instances of infringement does not render the red flag provision superfluous. The phrase “actual knowledge,” which appears in § 512(c)(1)(A)(i), is frequently used to denote subjective belief. [...] By contrast, courts often invoke the language of “facts or circumstances,” which appears in § 512(c)(1)(A)(ii), in discussing an objective reasonableness standard. [...]
- 43 The difference between actual and red flag knowledge is thus not between specific and generalized knowledge, but instead between a subjective and an objective standard. In other words, the actual knowledge provision turns on whether the provider actually or “subjectively” knew of specific infringement, while the red flag provision turns on whether the provider was subjectively aware of facts that would have made the specific infringement “objectively” obvious to a reasonable person. The red flag provision, because it incorporates an objective standard, is not swallowed up by the actual knowledge provision under our construction of the § 512(c) safe harbor. Both provisions do independent work, and both apply only to specific instances of infringement.

- 44 The limited body of case law interpreting the knowledge provisions of the § 512(c) safe harbor comports with our view of the specificity requirement. Most [676 F.3d 32] recently, a panel of the Ninth Circuit addressed the scope of § 512(c) in *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 667 F.3d 1022 (9th Cir.2011), a copyright infringement case against Veoh Networks, a video-hosting service similar to YouTube.<sup>[8]</sup> As in this case, various music publishers brought suit against the service provider, claiming direct and secondary copyright infringement based on the presence of unauthorized content on the website, and the website operator sought refuge in the § 512(c) safe harbor. The Court of Appeals affirmed the district court's determination on summary judgment that the website operator was entitled to safe harbor protection. With respect to the actual knowledge provision, the panel declined to "adopt[ ] a broad conception of the knowledge requirement," [...] holding instead that the safe harbor "[r]equir[es] specific knowledge of particular infringing activity;" [...]. The Court of Appeals "reach[ed] the same conclusion" with respect to the red flag provision, noting that "[w]e do not place the burden of determining whether [materials] are actually illegal on a service provider." [...].
- 45 Although *Shelter Capital* contains the most explicit discussion of the § 512(c) knowledge provisions, other cases are generally in accord. [...]
- 46 Based on the text of § 512(c)(1)(A), as well as the limited case law on point, we affirm the District Court's holding that actual knowledge or awareness of facts or circumstances that indicate specific and identifiable instances of infringement will disqualify a service provider from the safe harbor.
- 47 **2. The Grant of Summary Judgment**
- 48 The corollary question on appeal is whether, under the foregoing construction of § 512(c)(1)(A), the District Court erred in granting summary judgment to YouTube on the record presented. For the reasons that follow, we hold that although the District Court correctly interpreted § 512(c)(1)(A), summary judgment for the defendants was premature.
- 49 **i. Specific Knowledge or Awareness**
- 50 The plaintiffs argue that, even under the District Court's construction of the safe harbor, the record raises material issues of fact regarding YouTube's actual knowledge or "red flag" awareness of specific instances of infringement. To that end, the plaintiffs draw our attention to various estimates regarding the percentage of infringing content on the YouTube website. For example, Viacom cites evidence [676 F.3d 33] that YouTube employees conducted website surveys and estimated that 75–80% of all YouTube streams contained copyrighted material. The class plaintiffs similarly claim that Credit Suisse, acting as financial advisor to Google, estimated that more than 60% of YouTube's content was "premium" copyrighted content—and that only 10% of the premium content was authorized. These approximations suggest that the defendants were conscious that significant quantities of material on the YouTube website were infringing. [...] But such estimates are insufficient, standing alone, to create a triable issue of fact as to whether YouTube actually knew, or was aware of facts or circumstances that would indicate, the existence of particular instances of infringement.

- 51 Beyond the survey results, the plaintiffs rely upon internal YouTube communication: that do refer to particular clips or groups of clips. The class plaintiffs argue that YouTube was aware of specific infringing material because, *inter alia*, YouTube attempted to search for specific Premier League videos on the site in order to gauge their “value based on video usage.” In particular, the class plaintiffs cite a February 7, 2007 e-mail from Patrick Walker, director of video partnerships for Google and YouTube, requesting that his colleagues calculate the number of daily searches for the terms “soccer,” “football,” and “Premier League” in preparation for a bid on the global rights to Premier League content. On another occasion, Walker requested that any “clearly infringing, official broadcast footage” from a list of top Premier League clubs—including Liverpool Football Club, Chelsea Football Club, Manchester United Football Club, and Arsenal Football Club—be taken down in advance of a meeting with the heads of “several major sports teams and leagues.” YouTube ultimately decided not to make a bid for the Premier League rights—but the infringing content allegedly remained on the website.
- 52 The record in the Viacom action includes additional examples. For instance, YouTube founder Jawed Karim prepared a report in March 2006 which stated that, “[a]s of today[] episodes and clips of the following well-known shows can still be found [on YouTube]: Family Guy, South Park, MTV Cribs, Daily Show, Reno 911, [and] Dave Chapelle [sic].” Karim further opined that, “although YouTube is not legally required to monitor content ... and complies with DMCA takedown requests, we would benefit from preemptively removing content that is blatantly illegal and likely to attract criticism.” He also noted that “a more thorough analysis” of the issue would be required. At least some of the TV shows to which Karim referred are owned by Viacom. A reasonable juror could conclude from the March 2006 report that Karim knew of the presence of Viacom-owned material on YouTube, since he presumably located specific clips of the shows in question before he could announce that YouTube hosted the content “[a]s of today.” A reasonable juror could also conclude that Karim believed the clips he located to be infringing (since he refers to them as “blatantly illegal”), and that YouTube did not remove the content from the website until conducting “a more thorough analysis,” thus exposing the company to liability in the interim.
- 53 Furthermore, in a July 4, 2005 e-mail exchange, YouTube founder Chad Hurley sent an e-mail to his co-founders with the subject line “bndlight commercials,” and stated, “we need to reject these too.” Steve Chen responded, “can we please [676 F.3d 34] leave these in a bit longer? another week or two can't hurt.” Karim also replied, indicating that he “added back in all 28 bnd videos.” Similarly, in an August 9, 2005 e-mail exchange, Hurley urged his colleagues “to start being diligent about rejecting copyrighted / inappropriate content,” noting that “there is a cnn clip of the shuttle clip on the site today, if the boys from Turner would come to the site, they might be pissed?” Again, Chen resisted:
- 54 but we should just keep that stuff on the site. i really don't see what will happen. what? someone from cnn sees it? he happens to be someone with power? he happens to want to take it down right away. he gets in touch with cnn legal. 2 weeks later, we get a cease & desist letter. we take the video down.

And again, Karim agreed, indicating that “the CNN space shuttle clip, I like. we can remove it once we’re bigger and better known, but for now that clip is fine.”

- 55 Upon a review of the record, we are persuaded that the plaintiffs may have raised a material issue of fact regarding YouTube’s knowledge or awareness of specific instances of infringement. The foregoing Premier League e-mails request the identification and removal of “clearly infringing, official broadcast footage.” The March 2006 report indicates Karim’s awareness of specific clips that he perceived to be “blatantly illegal.” Similarly, the Bud Light and space shuttle e-mails refer to particular clips in the context of correspondence about whether to remove infringing material from the website. On these facts, a reasonable juror could conclude that YouTube had actual knowledge of specific infringing activity, or was at least aware of facts or circumstances from which specific infringing activity was apparent. See § 512(c)(1)(A)(i)-(ii). Accordingly, we hold that summary judgment to YouTube on all clips-in-suit, especially in the absence of any detailed examination of the extensive record on summary judgment, was premature.<sup>[9]</sup>
- 56 We hasten to note, however, that although the foregoing e-mails were annexed as exhibits to the summary judgment papers, it is unclear whether the clips referenced therein are among the current clips-in-suit. By definition, only the current clips-in-suit are at issue in this litigation. Accordingly, we vacate the order granting summary judgment and instruct the District Court to determine on remand whether any specific infringements of which YouTube had knowledge or awareness correspond to the clips-in-suit in these actions.
- 57 ii. “Willful Blindness”
- 58 The plaintiffs further argue that the District Court erred in granting summary judgment to the defendants despite evidence that YouTube was “willfully blind” to specific infringing activity. On this issue of first impression, we consider the application of the common law willful blindness doctrine in the DMCA context.
- 59 “The principle that willful blindness is tantamount to knowledge is hardly novel.” *Tiffany (NJ) Inc. v. eBay, Inc.*, 600 F.3d 93, 110 n. 16 (2d Cir.2010) (collecting [676 F.3d 35] cases); see *In re Aimster Copyright Litig.*, 33,4 F.3d 643 (7th Cir.2003) (“Willful blindness is knowledge, in copyright law ... as it is in the law generally.”). A person is “willfully blind” or engages in “conscious avoidance” amounting to knowledge where the person “ ‘was aware of a high probability of the fact in dispute and consciously avoided confirming that fact.’ ” [...] Writing in the trademark infringement context, we have held that “[a] service provider is not ... permitted willful blindness. When it has reason to suspect that users of its service are infringing a protected mark, it may not shield itself from learning of the particular infringing transactions by looking the other way.” *Tiffany*, 600 F.3d at 109.
- 60 The DMCA does not mention willful blindness. As a general matter, we interpret a statute to abrogate a common law principle only if the statute “speak[s] directly to the question addressed by the common law.” [...] The relevant question, therefore, is whether the DMCA “speak[s] directly” to the principle of willful blindness. [...] The DMCA provision most relevant to the abrogation inquiry is § 512(m), which provides that safe harbor protection shall not be conditioned on “a service provider monitoring its service

or affirmatively seeking facts indicating infringing activity, except to the extent consistent with a standard technical measure complying with the provisions of subsection (i).” 17 U.S.C. § 512(m)(1). Section 512(m) is explicit: DMCA safe harbor protection cannot be conditioned on affirmative monitoring by a service provider. For that reason, § 512(m) is incompatible with a broad common law duty to monitor or otherwise seek out infringing activity based on general awareness that infringement may be occurring. That fact does not, however, dispose of the abrogation inquiry, as previously noted, willful blindness cannot be defined as an affirmative duty to monitor. See *Aina-Marshall*, 336 F.3d at 170 (holding that a person is “willfully blind” where he “was aware of a high probability of the fact in dispute and consciously avoided confirming that fact”). Because the statute does not “speak[] directly” to the willful blindness doctrine, § 512(m) limits—but does not abrogate—the doctrine. Accordingly, we hold that the willful blindness doctrine may be applied, in appropriate circumstances, to demonstrate knowledge or awareness of specific instances of infringement under the DMCA.

- 61 The District Court cited § 512(m) for the proposition that safe harbor protection does not require affirmative monitoring, [...] but did not expressly address the principle of willful blindness or its relationship to the DMCA safe harbor. As a result, whether the defendants made a “deliberate effort to avoid guilty knowledge,” [...] remains a fact question for the District Court to consider in the first instance on remand.<sup>[10]</sup>

#### B. Control and Benefit: § 512(c)(1)(B)

- 63 Apart from the foregoing knowledge provisions, the § 512(c) safe harbor provides that an eligible service provider must “not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity.” 17 U.S.C. § 512(c)(1)(B). The District Court addressed this issue in a single paragraph, quoting from § 512(c)(1)(B), the so-called “control and benefit” provision, and concluding that “[t]he ‘right and ability to control’ the activity requires knowledge of it, which must be item-specific.” [...] For the reasons that follow, we hold that the District Court erred by importing a specific knowledge requirement into the control and benefit provision, and we therefore remand for further fact-finding on the issue of control.

##### 64 1. “Right and Ability to Control” Infringing Activity

- 65 On appeal, the parties advocate two competing constructions of the “right and ability to control” infringing activity. 17 U.S.C. § 512(c)(1)(B). Because each is fatally flawed, we reject both proposed constructions in favor of a fact-based inquiry to be conducted in the first instance by the District Court.

- 66 The first construction, pressed by the defendants, is the one adopted by the District Court, which held that “the provider must know of the particular case before he can control it.” [...] The Ninth Circuit recently agreed, holding that “until [the service provider] becomes aware of specific unauthorized material, it cannot exercise its ‘power or authority’ over the specific infringing item. In practical terms, it does not have the kind of ability to control infringing activity the statute contemplates.” [...] The trouble with this construction is that importing a specific knowledge requirement into § 512(c)(1)(B)

renders the control provision duplicative of § 512(c)(1)(A). Any service provider that has item-specific knowledge of infringing activity and thereby obtains financial benefit would already be excluded from the safe harbor under § 512(c)(1)(A) for having specific knowledge of infringing material and failing to effect expeditious removal. No additional service provider would be excluded by § 512(c)(1)(B) that was not already excluded by § 512(c)(1)(A). Because statutory interpretations that render language superfluous are disfavored, [...] we reject the District Court's interpretation of the control provision.

- 67 The second construction, urged by the plaintiffs, is that the control provision codifies the common law doctrine of vicarious copyright liability. The common law imposes liability for vicarious copyright infringement “[w]hen the right and ability to supervise coalesce with an obvious and direct financial interest in the exploitation of copyrighted materials—even in the absence of actual knowledge that the copyright mono [poly] is being impaired.” *Shapiro, Bernstein & Co. v. H.L. Green Co.*, 316 F.2d 304, 307 (2d Cir.1963)[...]. To support their codification argument, the plaintiffs rely [676 F.3d 37] on a House Report relating to a preliminary version of the DMCA: “The ‘right and ability to control’ language ... codifies the second element of vicarious liability.... Subparagraph (B) is intended to preserve existing case law that examines all relevant aspects of the relationship between the primary and secondary infringer.” H.R.Rep. No. 105-551(I), at 26 (1998). In response, YouTube notes that the codification reference was omitted from the committee reports describing the final legislation, and that Congress ultimately abandoned any attempt to “embark[] upon a wholesale clarification” of vicarious liability, electing instead “to create a series of ‘safe harbors’ for certain common activities of service providers.” S.Rep. No. 105-190, at 19.
- 68 Happily, the future of digital copyright law does not turn on the confused legislative history of the control provision. The general rule with respect to common law codification is that when “Congress uses terms that have accumulated settled meaning under the common law, a court must infer, unless the statute otherwise dictates, that Congress means to incorporate the established meaning of those terms.” [...] Under the common law vicarious liability standard, “ ‘[t]he ability to block infringers’ access to a particular environment for any reason whatsoever is evidence of the right and ability to supervise.’ ” *Anista Records LLC v. Usenet.com, Inc.*, 633 F.Supp.2d 124, 157 (S.D.N.Y.2009) (alteration in original) (quoting *A & M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1023 (9th Cir.2001)). To adopt that principle in the DMCA context, however, would render the statute internally inconsistent. Section 512(c) actually presumes that service providers have the ability to “block ... access” to infringing material. [...] Indeed, a service provider who has knowledge or awareness of infringing material or who receives a takedown notice from a copyright holder is required to “remove, or disable access to, the material” in order to claim the benefit of the safe harbor. 17 U.S.C. § 512(c)(1)(A)(iii) & (C). But in taking such action, the service provider would—in the plaintiffs’ analysis—be admitting the “right and ability to control” the infringing material. Thus, the prerequisite to safe harbor protection under § 512(c)(1)(A)(iii) & (C) would at the same time be a disqualifier under § 512(c)(1)(B).
- 69 Moreover, if Congress had intended § 512(c)(1)(B) to be coextensive with vicarious liability, “the statute could have accomplished that result in a more direct manner.” [...]

- 70 It is conceivable that Congress ... intended that [service providers] which receive a financial benefit directly attributable to the infringing activity would not, under any circumstances, be able to qualify for the subsection (c) safe harbor. But if that was indeed their intention, it would have been far simpler and much more straightforward to simply say as much. [...]
- 71 In any event, the foregoing tension—elsewhere described as a “predicament”<sup>[11]</sup> and a “catch22”<sup>[12]</sup>—is sufficient to establish that the control provision “dictates” [676 F.3d 36] a departure from the common law vicarious liability standard[...]. Accordingly, we conclude that the “right and ability to control” infringing activity under § 512(c)(1)(B) “requires something more than the ability to remove or block access to materials posted on a service provider’s website.” [...] The remaining—and more difficult—question is how to define the “something more” that is required.
- 72 To date, only one court has found that a service provider had the right and ability to control infringing activity under § 512(c)(1)(B).<sup>[13]</sup> In *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F.Supp.2d 1146 (C.D.Cal.2002), the court found control where the service provider instituted a monitoring program by which user websites received “detailed instructions regard[ing] issues of layout, appearance, and content.” [...] The service provider also forbade certain types of content and refused access to users who failed to comply with its instructions. [...] Similarly, inducement of copyright infringement under *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913, 125 S.Ct. 2764, 162 L.Ed.2d 781 (2005), which “premises liability on purposeful, culpable expression and conduct,” [...] might also rise to the level of control under § 512(c)(1)(B). Both of these examples involve a service provider exerting substantial influence on the activities of users, without necessarily—or even frequently—acquiring knowledge of specific infringing activity.
- 73 In light of our holding that § 512(c)(1)(B) does not include a specific knowledge requirement, we think it prudent to remand to the District Court to consider in the first instance whether the plaintiffs have adduced sufficient evidence to allow a reasonable jury to conclude that YouTube had the right and ability to control the infringing activity and received a financial benefit directly attributable to that activity.

#### C. “By Reason of” Storage: § 512(c)(1)

- 75 The § 512(c) safe harbor is only available when the infringement occurs “by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider.” 17 U.S.C. § 512(c)(1). In this case, the District Court held that YouTube’s software functions fell within the safe harbor for infringements that occur “by reason of” user storage. [...] For the reasons that follow, we affirm that holding [676 F.3d 39] with respect to three of the challenged software functions—the conversion (or “transcoding”) of videos into a standard display format, the playback of videos on “watch” pages, and the “related videos” function. We remand for further fact-finding with respect to a fourth software function, involving the third-party syndication of videos uploaded to YouTube.

- 76 As a preliminary matter, we note that “the structure and language of OCILLA indicate that service providers seeking safe harbor under [§ ] 512(c) are not limited to merely storing material.” [...] The structure of the statute distinguishes between so-called “conduit only” functions under § 512(a) and the functions addressed by § 512(c) and the other subsections. See 17 U.S.C. § 512(a) (“Subsections (a), (b), (c), and (d) describe separate and distinct functions for purposes of applying this section.”). Most notably, OCILLA contains two definitions of “service provider.” 17 U.S.C. § 512(k)(1)(A)-(B). The narrower definition, which applies only to service providers falling under § 512(a), is limited to entities that “offer[] the transmission, routing or providing of connections for digital online communications, between or among points specified by a user, of material of the user’s choosing, without modification to the content of the material as sent or received.” *Id.* § 512(k)(1)(A) (emphasis added). No such limitation appears in the broader definition, which applies to service providers—including YouTube—falling under § 512(c). Under the broader definition, “the term ‘service provider’ means a provider of online services or network access, or the operator of facilities therefor, and includes an entity described in subparagraph (A).” *Id.* § 512(k)(1)(B). In the absence of a parallel limitation on the ability of a service provider to modify user-submitted material, we conclude that § 512(c) “is clearly meant to cover more than mere electronic storage lockers.” [...]
- 77 The relevant case law makes clear that the § 512(c) safe harbor extends to software functions performed “for the purpose of facilitating access to user-stored material.” [...] Two of the software functions challenged here—transcoding and playback—were expressly considered by our sister Circuit in *Shelter Capital*, which held that liability arising from these functions occurred “by reason of the storage at the direction of a user.” [...] Transcoding involves “[m]aking copies of a video in a different encoding scheme” in order to render the video “viewable over the Internet to most users.” [...] The playback process involves “deliver[ing] copies of YouTube videos to a user’s browser cache” in response to a user request. [...] The District Court correctly found that to exclude these automated functions from the safe harbor would eviscerate the protection afforded to service providers by § 512(c). [...]
- 78 A similar analysis applies to the “related videos” function, by which a YouTube computer algorithm identifies and displays “thumbnails” of clips that are “related” to the video selected by the user. The plaintiffs claim that this practice constitutes content promotion, not “access” to stored content, and therefore falls beyond the scope of the safe harbor. Citing similar language in the Racketeer Influenced and Corrupt Organizations Act (“RICO”), 18 U.S.C. §§ 1961–68, and the Clayton [676 F.3d 40] Act, 15 U.S.C. §§ 12 et seq., the plaintiffs argue that the statutory phrase “by reason of” requires a finding of proximate causation between the act of storage and the infringing activity. [...] But even if the plaintiffs are correct that § 512(c) incorporates a principle of proximate causation—a question we need not resolve here—the indexing and display of related videos retain a sufficient causal link to the prior storage of those videos. The record makes clear that the related videos algorithm “is fully automated and operates solely in response to user input without the active involvement of YouTube employees.” [...] Furthermore, the related videos function serves to help YouTube users locate and gain access to material stored at the direction of other users. Because the algorithm “is closely related to, and follows from, the storage itself,” and is “narrowly directed toward providing access to material stored at

the direction of users,” [...] we conclude that the related videos function is also protected by the § 512(c) safe harbor.

- 79 The final software function at issue here—third-party syndication—is the closest case. In or around March 2007, YouTube transcoded a select number of videos into a format compatible with mobile devices and “syndicated” or licensed the videos to Verizon Wireless and other companies. The plaintiffs argue—with some force—that business transactions do not occur at the “direction of a user” within the meaning of § 512(c)(1) when they involve the manual selection of copyrighted material for licensing to a third party. The parties do not dispute, however, that none of the clips-in-suit were among the approximately 2,000 videos provided to Verizon Wireless. In order to avoid rendering an advisory opinion on the outer boundaries of the storage provision, we remand for fact-finding on the question of whether any of the clips-in-suit were in fact syndicated to any other third party.

#### D. Other Arguments

##### 81 1. Repeat Infringer Policy

- 82 The class plaintiffs briefly argue that YouTube failed to comply with the requirements of § 512(i), which conditions safe harbor eligibility on the service provider having “adopted and reasonably implemented ... a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider’s system or network who are repeat infringers.” 17 U.S.C. § 512(i)(1)(A). Specifically, the class plaintiffs allege that YouTube “deliberately set up its identification tools to try to avoid identifying infringements of class plaintiffs’ works.” This allegation rests primarily on the assertion that YouTube permitted only designated “partners” to gain access to content identification tools by which YouTube would conduct network searches and identify infringing material.[14]

- 83 Because the class plaintiffs challenge YouTube’s deployment of search technology, [676 F.3d 41] we must consider their § 512(i) argument in conjunction with § 512(m). As previously noted, § 512(m) provides that safe harbor protection cannot be conditioned on “a service provider monitoring its service or affirmatively seeking facts indicating infringing activity, except to the extent consistent with a standard technical measure complying with the provisions of subsection (i).” 17 U.S.C. § 512(m)(1) (emphasis added). In other words, the safe harbor expressly disclaims any affirmative monitoring requirement—except to the extent that such monitoring comprises a “standard technical measure” within the meaning of § 512(i). Refusing to accommodate or implement a “standard technical measure” exposes a service provider to liability, refusing to provide access to mechanisms by which a service provider affirmatively monitors its own network has no such result. In this case, the class plaintiffs make no argument that the content identification tools implemented by YouTube constitute “standard technical measures,” such that YouTube would be exposed to liability under § 512(i). For that reason, YouTube cannot be excluded from the safe harbor by dint of a decision to restrict access to its proprietary search mechanisms.

84 **2. Affirmative Claims**

85 Finally, the plaintiffs argue that the District Court erred in denying summary judgment to the plaintiffs on their claims of direct infringement, vicarious liability, and contributory liability under *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913, 125 S.Ct. 2764, 162 L.Ed.2d 781 (2005). In granting summary judgment to the defendants, the District Court held that YouTube “qualif[ie]d for the protection of ... § 512(c),” and therefore denied the plaintiffs’ cross-motion for summary judgment without comment. [...]

86 The District Court correctly determined that a finding of safe harbor application necessarily protects a defendant from all affirmative claims for monetary relief. 17 U.S.C. § 512(c)(1)[...]. For the reasons previously stated, further fact-finding is required to determine whether YouTube is ultimately entitled to safe harbor protection in this case. Accordingly, we vacate the order denying summary judgment to the plaintiffs and remand the cause without expressing a view on the merits of the plaintiffs’ affirmative claims.

### CONCLUSION

88 To summarize, we hold that:

89 (1) The District Court correctly held that 17 U.S.C. § 512(c)(1)(A) requires knowledge or awareness of facts or circumstances that indicate specific and identifiable instances of infringement;

(2) However, the June 23, 2010 order granting summary judgment to YouTube is **VACATED** because a reasonable jury could conclude that YouTube had knowledge or awareness under § 512(c)(1)(A) at least with respect to a handful of specific clips; the cause is **REMANDED** for the District Court to determine whether YouTube had knowledge or awareness of any specific instances of infringement corresponding to the clips-in-suit;

(3) The willful blindness doctrine may be applied, in appropriate circumstances, to demonstrate knowledge or awareness of specific instances of infringement under § 512(c)(1)(A); the cause is **REMANDED** for the [676 F.3d 42] District Court to consider the application of the willful blindness doctrine in the first instance;

(4) The District Court erred by requiring “item-specific” knowledge of infringement in its interpretation of the “right and ability to control” infringing activity under 17 U.S.C. § 512(c)(1)(B), and the judgment is **REVERSED** insofar as it rests on that erroneous construction of the statute; the cause is **REMANDED** for further fact-finding by the District Court on the issues of control and financial benefit;

(5) The District Court correctly held that three of the challenged YouTube software functions—replication, playback, and the related videos feature—occur “by reason of the storage at the direction of a user” within the meaning of 17 U.S.C. § 512(c)(1), and the judgment is **AFFIRMED** insofar as it so held; the cause is **REMANDED** for further fact-finding regarding a fourth software function,

involving the syndication of YouTube videos to third parties.

On remand, the District Court shall allow the parties to brief the following issues, with a view to permitting renewed motions for summary judgment as soon as practicable:

- (A) Whether, on the current record, YouTube had knowledge or awareness of any specific infringements (including any clips-in-suit not expressly noted in this opinion);
- (B) Whether, on the current record, YouTube willfully blinded itself to specific infringements;
- (C) Whether YouTube had the “right and ability to control” infringing activity within the meaning of § 512(c)(1)(B); and
- (D) Whether any clips-in-suit were syndicated to a third party and, if so, whether such syndication occurred “by reason of the storage at the direction of the user” within the meaning of § 512(c)(1), so that YouTube may claim the protection of the § 512(c) safe harbor.

We leave to the sound discretion of the District Court the question of whether some additional, guided discovery is appropriate in order to resolve “(C)” (“[w]hether YouTube had ‘the right and ability to control’ infringing activity”), and “(D)” (“[w]hether any clips-in-suit were syndicated to a third party”). As noted above, for purposes of this case, the record with respect to “(A)” (“[w]hether ... YouTube had knowledge or awareness of any specific infringements”) and “(B)” (“[w]hether YouTube willfully blinded itself to specific infringements”) is now complete.

90 Each party shall bear its own costs.[...]

[Notes:]

- 97 [4] The “Flash” format “is a highly compressed streaming format that begins to play instantly. Unlike other delivery methods, it does not require the viewer to download the entire video file before viewing.” Joint App’n IV:73.
- 98 [5] Doctrines of secondary copyright infringement include contributory, vicarious, and inducement liability. See *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913, 930–31, 936–37, 125 S.Ct. 2764, 162 L.Ed.2d 781 (2005).[...]
- 100 [7] It is undisputed that all clips-in-suit had been removed from the YouTube website by the time of summary judgment, mostly in response to DMCA takedown notices. *Viacom Int’l*, 718 F.Supp.2d at 519.[...]
- 102 [9] We express no opinion as to whether the evidence discussed above will prove sufficient to withstand a renewed motion for summary judgment by YouTube on remand.

In particular, we note that there is at least some evidence that the search requested by Walker in his February 7, 2007 e-mail was never carried out. See Joint App'x III:256. We also note that the class plaintiffs have failed to identify evidence indicating that any infringing content discovered as a result of Walker's request in fact remained on the YouTube website. The class plaintiffs, drawing on the voluminous record in this case, may be able to remedy these deficiencies in their briefing to the District Court on remand.

- 103 [10] Our recent decision in *Tiffany (NJ) Inc. v. eBay Inc.*, 600 F.3d 93 (2d Cir.2010), lends support to this result. In *Tiffany*, we rejected a willful blindness challenge, holding that although eBay “knew as a general matter that counterfeit Tiffany products were listed and sold through its website,” such knowledge “is insufficient to trigger liability.” *Id.* at 110. In so holding, however, we rested on the extensive findings of the district court with respect to willful blindness. *Id.* (citing *Tiffany (NJ) Inc. v. eBay, Inc.*, 576 F.Supp.2d 463, 513 (S.D.N.Y.2008)). Thus, the *Tiffany* holding counsels in favor of explicit fact-finding on the issue of willful blindness.[...]
- 106 [13] Other courts have suggested that control may exist where the service provider is “actively involved in the listing, bidding, sale and delivery” of items offered for sale, *Hendrickson v. eBay, Inc.*, 165 F.Supp.2d 1062, 1094 (C.D.Cal.2001), or otherwise controls vendor sales by previewing products prior to their listing, editing product descriptions, or suggesting prices, *Corbis Corp.*, 351 F.Supp.2d at 1110. Because these cases held that control did not exist, however, it is not clear that the practices cited therein are individually sufficient to support a finding of control.[...]

***Caso 3– Waymo***

(Vide nota de rodapé nº 40)

## **ANEXO D – Pesquisa Internacional**

### **ANEXO D – Pesquisa realizada (âmbito nacional e internacional)**

#### ***Metodologia***

Aplicação de método empírico, com aplicação de 2 tipos de questionário: (1) entrevista presencial; (2) entrevista por e-mail.

#### ***Modelo de Questionário (1): verbal***

1. Qual sua opinião sobre uma regulamentação internacional para a Internet?
2. A Internet deveria ser governada por contratos como do Facebook?
3. Como fica a proteção da propriedade intelectual das bases de dados das empresas (o que elas passam a saber a partir do que fabricam IOT)?
4. Podemos chamar de propriedade se com a proteção de dados pessoais seria revogável?  
Tem que ser excluído?

#### ***Modelo de Questionário (2): por e-mail***

1. Você acha que a legislação em vigor sobre Propriedade intelectual sobre bases de dados (no Brasil) é suficiente para proteger este ativo em um cenário completo de bases de dados digitais coletadas via internet e dados industriais coletados via internet das coisas? Por exemplo, se um caso que possui IoT, cuja caixa preta pode coletar dados do carro, e também do motorista, a quem pertence a Propriedade dos dados coletados? Pertencem naturalmente ao fabricante do carro? Ao proprietário do veículo? Ao motorista que está conduzindo? De quem é o direito sobre os dados? Que direito seria este? Propriedade intelectual, *sui generis*, privacidade, outro tipo? E depende do que? Depende do tipo de dado coletado? Depende do tipo de contrato estabelecido? E o que pode ser feito com os dados coletados (seria ilimitado ou limitado)?
2. Você acha que a natureza globalizada da internet exige que haja uma regulamentação internacional sobre a Propriedade intelectual das bases de dados digitais coletadas via internet e das bases industriais coletadas via IoT, tendo em vista a necessidade crescente de harmonizar estes direitos de Propriedade com as novas regulamentações que tem surgido sobre Privacidade e Proteção de Dados Pessoais em níveis Nacionais e Regionais (em vários países)?
3. Você acha que Propriedade intelectual das bases de dados digitais coletadas via internet e das bases industriais coletadas via IoT deveriam ser regidas apenas por contratos (sem necessidade de uma legislação específica nacional ou um tratado internacional)? Seria suficiente? E estes contratos poderiam ter qualquer tipo de cláusula ou deveriam seguir um modelo (como por exemplo o da Directiva 97/7/CE and 93/13/CEE sobre cláusulas abusivas).

***Professores entrevistados (entrevista verbal):***

## Lista de professores

- (1) Prof. Albert Gidari (Universidade de Stanford – Centro de Internet e Sociedade - EUA)
- (2) Alexandre Dias Pereira (Universidade de Coimbra – Portugal)
- (3) Ann Bartow (Faculdade de Direito da Universidade de New Hampshire - EUA)
- (4) Prof. Antonio Carlos Morato (Universidade de São Paulo - Brasil)
- (5) Prof. Chris Reed (Universidade Queen Mary de London - Inglaterra)
- (6) Prof. Daphne Keller (Universidade de Stanford - EUA)
- (7) Dario Moura Vicente (Universidade de Lisboa - Portugal)
- (8) Eike Hosemann (Max Planck Institute de Hamburgo - Alemanha)
- (9) Gerald Splindler (Universidade de Gottingen - Alemanha)
- (10) Gloria Gonzales Fuster (Universidade de Bruxelas - Bélgica)
- (11) Jacqueline Lipton (Universidade de Akron - EUA)
- (12) Jan Luttrinhaus (Max Planck Institute de Hamburgo - Alemanha)
- (13) Jan Schmidt (Max Planck Institute de Hamburgo - Alemanha)
- (14) Prof. Jeremy Malcolm (Electronic Frontier Foundation – EFF - EUA)
- (15) Prof. Josef Drexler (Max Planck Institute de Munique – Alemanha)
- (16) June Besek (Universidade de Columbia - EUA)
- (17) Luis Filipe Antunes (Universidade do Porto - Portugal)
- (18) Nathália Mazonetto (Universidade de São Paulo – Brasil)
- (19) Nicholas Hernanz (Deputado do Partido The Greens – Parlamento Europeu - Bélgica)
- (20) Rafael Ferraz Vazques (World Intellectual Property Organization - WIPO - Suíça)
- (21) Reinhard Zimmermann (Max Planck Institute de Hamburgo - Alemanha)
- (22) Remédio Marques (Universidade de Coimbra - Portugal)
- (23) Reto M. Hilty (Max Planck Institute de Munique - Alemanha)
- (24) Prof. Rolf Weber (Universidade de Zurich - Suíça)
- (25) Roya Ghafele (Universidade de Oxford - Inglaterra)
- (26) Valentina Moscon (Max Planck Institute de Munique - Alemanha)
- (27) Wolf Meier-Ewert (World Trade Organization - WTO - Suíça)

***Professores entrevistados (entrevista pessoal por e-mail<sup>296</sup>):***

Albert Gidari (Universidade de Stanford – Centro de Internet e Sociedade - EUA)

**From:** Albert Gidari [mailto: [REDACTED]]  
**Sent:** Thursday, June 15, 2017 6:40 PM  
**To:** Patricia Pinheiro <patricia.peck@peckadvogados.com.br>  
**Subject:** Re: invite to participate on PhD research - Patricia Peck from São Paulo University with Columbia University and Max Planck Institute - Intellectual Property and Privacy

Alexandre Dias Pereira (Universidade de Coimbra – Portugal)

**From:** Alexandre Dias Pereira [mailto: [REDACTED]]  
**Sent:** Friday, July 7, 2017 11:22 AM  
**To:** Patricia Pinheiro <patricia.peck@peckadvogados.com.br>  
**Subject:** RE: contato Prof. Patricia Peck Pinheiro Universidade de São Paulo - pesquisa da Tese – convite

Ann Bartow (Faculdade de Direito da Universidade de New Hampshire - EUA)

**From:** Bartow, Ann [mailto: [REDACTED]]  
**Sent:** Monday, July 10, 2017 1:58 PM  
**To:** Patricia Pinheiro <patricia.peck@peckadvogados.com.br>  
**Subject:** RE: Virtual Introduction

Antonio Carlos Morato (Universidade de São Paulo - Brasil)

**From:** Antonio Carlos Morato [mailto: [REDACTED]]  
**Sent:** Monday, June 26, 2017 9:11 AM  
**To:** Patricia Pinheiro <patricia.peck@peckadvogados.com.br>  
**Subject:** Tese de doutorado – questionário

Chris Reed (Universidade Queen Mary de London - Inglaterra)

**From:** Chris Reed [mailto: [REDACTED]]  
**Sent:** Monday, June 26, 2017 11:15 AM  
**To:** Patricia Pinheiro <patricia.peck@peckadvogados.com.br>  
**Subject:** Re: request to participate in the research - Patricia Peck - cyber law attorney from Brazil (Phd visiting researcher at Columbia University and Max Planck Institute)

---

<sup>296</sup>Em atenção à regulamentação de proteção de dados da União Europeia (GDPR) em vigor, os endereços de emails foram removidos.

Daphne Keller (Universidade de Stanford - EUA)

**From:** Daphne Keller [mailto: [REDACTED]]  
**Sent:** Monday, June 12, 2017 2:59 PM  
**To:** Patricia Pinheiro <patricia.peck@peckadvogados.com.br>  
**Subject:** Re: invite to participate on PhD research - Patricia Peck from São Paulo University with Columbia University and Max Planck Institute - Intellectual Property and Privacy

Jeremy Malcolm (Electronic Frontier Foundation – EFF - EUA)

**From:** Jeremy Malcolm [mailto: [REDACTED]]  
**Sent:** Thursday, June 22, 2017 8:04 PM  
**To:** Patricia Pinheiro <patricia.peck@peckadvogados.com.br>  
**Subject:** Re: invite to participate on PhD research - Patricia Peck from São Paulo University with Columbia University and Max Planck Institute - Intellectual Property and Privacy

Josef Drexl (Max Planck Institute de Munique – Alemanha)

**From:** Drexl Josef [mailto: [REDACTED]]  
**Sent:** Monday, June 12, 2017 5:14 PM  
**To:** Patricia Pinheiro <patricia.peck@peckadvogados.com.br>  
**Subject:** RE: Meeting request - Patricia Peck aus Brasilien. - my questions for the PhD research

Nathália Mazonetto (Universidade de São Paulo – Brasil)

**From:** Nathalia Mazzonetto | MommaLaw [mailto: [REDACTED]]  
**Sent:** Monday, June 19, 2017 11:10 AM  
**To:** Patricia Pinheiro <patricia.peck@peckadvogados.com.br>  
**Subject:** RES: contato com a Prof. Natália Mazoneto - Patricia Peck (Universidade de Sao Paulo, Columbia University e Max Planck Institute) - por indicação Prof. Remédio Marques Universidade Coimbra

Rolf Weber (Universidade de Zurich - Suíça)

**From:** Weber Rolf [mailto: [REDACTED]]  
**Sent:** Saturday, June 17, 2017 8:46 AM  
**To:** Patricia Pinheiro <patricia.peck@peckadvogados.com.br>  
**Subject:** WG: request for a meeting - Patricia Peck - cyber law attorney from Brazil (Phd visiting researcher at Columbia University)