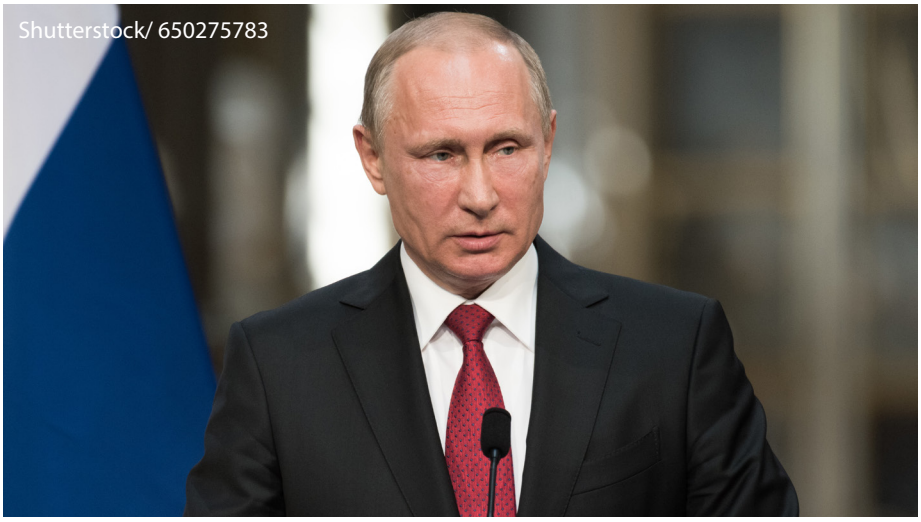
MEDIA LAW INTERNATIONAL ®

e-Zine 06/19

President Putin signs law to impose fines on print media


Shutterstock/ 650275783

Russia introduces new law prohibiting the production and distribution of foreign print media without permits

President Vladimir Putin signed a new law on 17 June that imposes fines for the unathorised production or distribution of foreign print media.

The law requires media publications to register their media outlet with the Russian media regulator Roskomnadzor, and obtain a permit.

The legal change is intended to improve regulation of foreign media outlets that have contracts with local distributors, and ensure that such contracts are brought under the review of the state.

The President's Executive Office published an update on its website, stating 'The production or distribution of unregistered media products, including the unauthorised distribution of foreign print media products in the Russian Federation, is now an administrative offence.'

The law states that the publication or distribution of foreign media publications, without a permit, will be subject to fines.

The new rules apply to individuals as well as media outlets, with fines up to RUB30,000 (USD470) for media corporations. ➔

Landmark ruling on 'serious harm' in defamation law

A landmark court ruling in the UK has clarified 'serious harm' in a defamation law, while raising the bar for new claims.

The Supreme Court issued a ruling on 12 June against the Independent and Evening Standard in a libel case that involved articles published in 2014 about the marriage breakdown of engineer Bruno Lachaux.

The court found that published articles caused serious harm. The court addressed the threshold of 'serious harm' in Section 1 of the Defamation Act 2013 in a case that is the first to reach the Supreme Court.

In July 2015, the High Court ruled in favour of Mr Lachaux. The ruling was appealed in September 2017 but later upheld by the Court of Appeal.

The Supreme Court found that Section 1 of the Act "raises the threshold of seriousness" above that of case law prior to the Act, and "requires its application to be determined by reference to the actual facts about [the statement in question's] impact and not just to the meaning of the words".

Lawyer Alex Keenlyside, Pinsent Masons, commented that the ruling is likely to make it more difficult for claimants to bring successful libel claims.

In an article published by the law firm, Mr Keenlyside said:

"The challenge for judges now is to find a way of managing cases efficiently such that in appropriate cases the 'serious harm' point can be tested at an early stage in proceedings, rather than at trial when all of that time and cost has been incurred." ■

What's inside

Contact
Zineb Serroukh-Ouarda
Managing Editor
zserroukh@medialawinternational.com
+44 7446 525 299

Contributors

CAHILL GORDON & REINDEL LLP

LAWPLUS LawPlus Ltd.

ringier axel springer

US private equity firm KKR agrees to buy Axel Springer, Germany's largest publisher

Us private equity firm KKR has agreed to buy Germany's biggest publisher Axel Springer in a GBP6 billion investor agreement that supports long-term growth.

KKR's voluntary public tender offer was announced on 12 June at rate of EUR63.00 per share in cash.

The deal follows Axel Springer's growth strategy review, initiated by its Executive Board in December 2018. KKR's share offer represented a premium of 40 per cent to Axel Springer's unaffected share price.

The investor agreement also states that editorial independence at Axel Springer will be preserved.

Mathias Döpfner, CEO of Axel Springer, said: "The strategic partnership with KKR would enable us to pursue major growth opportunities by providing additional financial capabilities while relieving the mere focus on short-term financial targets.

He added: "KKR is a long-term focused partner who respects and supports our commitment to independent journalism."

Both companies expect the deal to strengthen Axel Springer's position in challenging markets. In a press release, KKR commented: 'KKR sees opportunities to further develop Axel Springer and to strengthen its market position.' ■

China-Russia cooperation set to strengthen media

Leaders of the Shanghai Cooperation Organisation (SCO) countries have signed an agreement on mass media cooperation with the Russia.

The agreement was signed on 14 June by Russian Deputy Minister of Communications, Alexander Volin, and allows for greater cooperation among SCO member countries. It also allows Russia to expand its cooperation within the SCO.

Mr Volin issued a statement confirming: 'Among other things, the document envisages creating favorable conditions for large-scale mutual dissemination of information, mutually beneficial cooperation among editorial boards of media from participating states, exchange of professional experience, holding meetings, seminars and conferences devoted to the media sector, mutual assistance to TV and radio broadcasting, work of news bureaus, training of specialists.'

The SCO is an intergovernmental international organisation, established in 2001 by leaders of China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan and Uzbekistan.

China-Russia relations have strengthened over the past year, with senior Chinese officials calling on media from both countries to enhance the development of bilateral ties.

During the fourth China-Russia Media Forum in Shanghai, held on 04 November last year, Huang Kunming, member of the Political Bureau of the Communist Party of China, said strategic partnership between both countries is the best it has been in history. ■

President Putin signs law to fines print media

continued from page 1

← Individuals who distribute unauthorised foreign print media will be subject to fine of up to RUB1,500 USD23).

The draft legislation was first considered by the State Duma, the lower chamber of the Russian parliament, on 02 April 2019 before being signed into law.

The Committee to Protect Journalists commented on the development, stating 'The amendments introduced in Russia's State Duma on April 2 show how authorities in Moscow are continuously scanning the landscape for new ways to tighten state control over news and information.'

The Committee to Protect Journalists added: 'We call on the Duma to drop these amendments and on Russian authorities to stop turning Roskomnadzor into a giant government censorship agency.'

In 2017, Mr Putin signed a law that allows prosecutors to categorise outlets that receive funding from abroad as 'foreign media'.

Industry lawyers say the law would affect print media sold within Russia as well as printed publications brought into the country by individuals.

The legislative change is expected to bring specific contracts between print media outlets and local distributors under Roskomnadzor's authority's. ■

The future of FCC media ownership rules in age of Netflix

Chérie R. Kiser

Managing partner Chérie R. Kiser outlines challenges of the platinum age of content

The Federal Communications Commission (FCC) media ownership rules were adopted in an era dominated by local radio and broadcast television, before the rise of the internet and cable news. The latest FCC review of those rules highlights how government regulators continue to struggle to keep pace with rapidly-changing communications technology and an exploding marketplace of consumer choices.

In 2018, the FCC issued its Quadrennial Regulatory Review Notice of Proposed Rulemaking, (2018 NPRM) announcing its latest review of its media ownership rules.

In an accompanying statement, FCC Commissioner Carr observed:

'Things have changed as today's Communications Marketplace Report notes, Netflix this year [2018] will spend more than USD8 billion on content, a quarter of which is for original shows. Amazon will spend USD5 billion, Hulu: USD3 billion. Next year [2019], Google is expected to earn USD48 billion in ad revenue, including in competition with broadcasters for local ad dollars. And Spotify and Pandora are increasingly competing for the ears of Americans whether we're at home or on the go.

The golden age of television – or the platinum age of content – is the direct result of choice. The gatekeepers of the past are no longer gatekeepers. Americans, using broadband connection, can access any content, from any device, anywhere.

As explained in the 2018 article in Media Law International, "Are the FCC Media Ownership Rules Still Relevant in the Digital Age?," the media ownership rules limit who may own a broadcast media outlet and how many outlets may be owned by the same entity in any given market. The regulations were designed to promote localism, diversity, and competition in the use of broadcast spectrum.

In its 1996 amendment to the Communications Act of 1934,Congress directed the FCC to review the media ownership rulesevery four years to determine whether they "are necessary in the public interest as a result of competition." Congress also directed the FCC to repeal or modify any regulation no longer in the public interest.

Every review since 2002 has been challenged in court, with those challenges taking years to resolve. The recent FCC Order on Reconsideration of the 2016 Second Report and Orderis no exception. The decision is on appeal to the Third Circuit by Prometheus Radio Project, which argues that the FCC failed to take diversity sufficiently into account.

Regardless of the outcome of the appeal in Prometheus Radio Project, the FCC's 2018NPRMis moving forward. Per the 2018NPRM, the FCCwill review three rules: Local Radio OwnershipRule, Local Television Ownership Rule, and the Dual Network Rule. Generally, these rules limit the number and/or type of radio/television stations that can be owned in a market. The 2018 NPRM reaches no tentative conclusions; instead it asks numerous questions and requests evidentiary support for positions taken.

In the 2018 NPRM, the presence of digital technologies such as streaming services, online distribution of programming from a variety of sources, and non-video providers of news and information such as Internet websites and social media appear likely to play a prominent part of the discussion during this review. It does seem apparent that technology may be rapidly outpacing the underlying facts and circumstances that led to the creation of the ownership rules in the first place, and the FCC hopes to respond accordingly. The only thing we can predict at this stage is that there will be more to report in 2020 – and likely more litigation to follow! ■

Chérie R. Kiser, Cahill Gordon & Reindel
CKiser@cahill.com
+1.202.862.8950

Thailand: Innovation Driven by Trust


Shutterstock/ 665143720

Kowit Somwaiya, Managing Partner at LawPlus, highlights the role of Thailand's Personal Data Protection Act and Cyber Security Act in industry development

As a country thought to be stuck in the "Middle Income Trap", Thailand is innovating its way out. The kingdom is shifting away from a manufacturing-based economy into one driven by innovation and technology through the government's 'Thailand 4.0' initiative.

A cornerstone of Thailand 4.0 is the need to cultivate trust in consumers and investors about the stability, sustainability and safety of Thailand's booming digital economy.

To this end, the Personal Data Protection Act B.E. 2562 (PDPA) and Cyber Security Act B.E. 2562 (CSA) have been enacted and are effective (in full for the CSA and in part for the PDPA) as of 28 May 2019.

The CSA aims to secure national security in cyber-space through the protection of Information Infrastructures (II), which the CSA deems critical or important such as public/private databases, computer systems and networks. Where the CSA applies to the safety of the underlying infrastructure of the Digital Economy, the PDPA concerns itself with the rights and protection of data subjects. It mandates that the explicit consent of a data subject must be sought by those collecting personal data prior to collection, use or disclosure.

Cyber Security Act

The CSA establishes a number of bodies that discharge the duties under this law. In particular, the National Cyber Security Committee (NCSC), the Cyber Security Governance Committee (NSGC), the Executive Committee of the Office of the Cyber Security Committee and the Office of the National Cyber Security Committee (ONCSC).

The CSA's main impact is its focus on protecting the kingdom's II from cyber security threats, therefore, ensuring the country's economy is well protected from highly disruptive cyber attacks.

The country accomplishes this by empowering the above mentioned committees to perform key responsibilities such as drafting and enforcing standards frameworks, codes of conduct and risk-assessment measures to ensure that Information Infrastructure Authorities (IIA), which manage IIs are adequately protected from any cyber security threats; and analysing cyber security related situations and assess their impacts to prevent, handle and mitigate cyber security threats in the future.

The CSA defines II as any computer, or computer system used by either government of private entities for operations which are related to national security, safety, economic stability or are public interest infrastructures.

This includes, but is not limited to, the provision of information infrastructure services in the following sectors: banking, IT/telecoms, energy and public utilities, transportation/logistics, and public health.

For example, a cloud provider whose server hosts important financial information from the banking sector on their servers or hosts highly sensitive patient records must comply with the kngdom's new cyber security laws.

IIAs must comply with the four key requirements under the CSA as follows:

1. Conduct cyber security risk assessments at least once a year and send a summary of said report to the ONCSC within 30 days of completion;

2. Create and implement sector specific mechanisms, procedures and codes of conduct which must at least adhere to the codes of conduct issued by the CSGC to monitor cyber security threats and solve cyber security issues;

3. Notify the ONCSC of the names and contact information of owners, possessors of the computer and the computer system's administrators; and

4. Report cyber security threats to the ONCSC where cyber security threats occur (failure to do so may result in a fine of up to THB200,000).

Thailand: Innovation Driven by Trust

Kowit Somwaiya,
Managing Parter, LawPlus

kowit.somwaiya@lawplusltd.com

+662 636 0662

www.lawplusltd.com

Unit 1401, 14th Floor,
Abdulrahim Place 990
Rama IV Road,
Bangkok 10500, Thailand

Personal Data Protection Act

The PDPA establishes a Personal Data Protection Commission (PDPC) and the Office of the PDPC (OPDPC) to ensure that Personal Data Controllers (Controllers) (those who have the power to control the collection, use or disclosure of collected personal data) and Personal Data Processors (Processors) (those who collect, use or discloses of personal data on behalf of a Personal Data Controller) comply with the PDPA.

The PDPA is extra-territorial and applies to Controllers and Processors both within Thailand and abroad where the data collected, used or disclosed is of a data subject within Thailand.

Controllers and Processors must be aware of the following key principles of the PDPA:

1. Explicit consent to collection, use or disclosure of personal data must be obtained from data subjects, by Controllers and Processors, subject to certain exceptions;

2. Personal data may only be collected, used or disclosed for lawful purposes which have been notified to the data subject and no more;

3. Controllers must also inform data subjects of the types of persons or authorities which the collected personal data will be disclosed to, information about said Controller and the rights of a data subject (e.g. the right to access, make copies of, raise objections, request destruction of data or revoke consent for the use of their personal data);

4. Data Protection Officers must be appointed by Controllers where required;

5. Controllers and Processors must provide appropriate measures to protect and secure collected personal data; and

6. Transfer of personal data to a foreign country or an international organization may only occur if such country or organization has a sufficient standard of personal data protection.

The PDPA also imports and adapts some concepts from the European Union's General Data Protection Regulation 2016/679 (GDPR). This includes concepts of data retention periods and data portability.

While the PDPA is now effective in part, its key provisions on data collection, use and disclosure, etc. are exempt from being effective until the 28th of May 2020 to allow businesses sufficient time to be fully prepared to comply with the PDPA.

The PDPC will issue rules before 28 May 2020 to implement the PDPA. Businesses in Thailand and abroad will need to monitor such rules and prepare to fully comply with the PDPA and its implementation rules.